

THE EMV DEADLINE AND WHAT IT MEANS FOR SMALL BUSINESSES: PART II

HEARING BEFORE THE COMMITTEE ON SMALL BUSINESS UNITED STATES HOUSE OF REPRESENTATIVES ONE HUNDRED FOURTEENTH CONGRESS FIRST SESSION

HEARING HELD
OCTOBER 21, 2015



Small Business Committee Document Number 114-026
Available via the GPO Website: www.fdsys.gov

U.S. GOVERNMENT PUBLISHING OFFICE

97-228

WASHINGTON : 2015

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

HOUSE COMMITTEE ON SMALL BUSINESS

STEVE CHABOT, Ohio, *Chairman*
STEVE KING, Iowa
BLAINE LUTKEMEYER, Missouri
RICHARD HANNA, New York
TIM HUELSKAMP, Kansas
TOM RICE, South Carolina
CHRIS GIBSON, New York
DAVE BRAT, Virginia
AUMUA AMATA COLEMAN RADEWAGEN, American Samoa
STEVE KNIGHT, California
CARLOS CURBELO, Florida
MIKE BOST, Illinois
CRESENT HARDY, Nevada
NYDIA VELÁZQUEZ, New York, *Ranking Member*
YVETTE CLARK, New York
JUDY CHU, California
JANICE HAHN, California
DONALD PAYNE, JR., New Jersey
GRACE MENG, New York
BRENDA LAWRENCE, Michigan
ALMA ADAMS, North Carolina
SETH MOULTON, Massachusetts
MARK TAKAI, Hawaii

KEVIN FITZPATRICK, *Staff Director*
STEPHEN DENIS, *Deputy Staff Director for Policy*
JAN OLIVER, *Deputy Staff Director for Operation*
BARRY PINELES, *Chief Counsel*
MICHAEL DAY, *Minority Staff Director*

CONTENTS

OPENING STATEMENTS

Hon. Steve Chabot	Page 1
Hon. Nydia Velázquez	2

WITNESSES

Ms. Jami Wade, Owner, Capitol City CORK and Provisions & Capitol City Cinema, Jefferson City, MO	4
Mr. Keith Lipert, Owner, Keith Lipert Gallery, Washington, DC, testifying on behalf of the National Retail Federation	6
Mr. Jared Scheeler, Managing Director, The Hub Convenience Stores, Inc., Dickinson, ND, testifying on behalf of National Association of Convenience Stores	8
Art Potash, CEO, Potash Markets, Chicago, IL, testifying on behalf of the Food Marketing Institute	9
Ed Mierzewski, Consumer Program Director and Senior Fellow, U.S. Public Interest Research Group, Washington, DC	10

APPENDIX

Prepared Statements:

Ms. Jami Wade, Owner, Capitol City CORK and Provisions & Capitol City Cinema, Jefferson City, MO	25
Mr. Keith Lipert, Owner, Keith Lipert Gallery, Washington, DC, testifying on behalf of the National Retail Federation	28
Mr. Jared Scheeler, Managing Director, The Hub Convenience Stores, Inc., Dickinson, ND, testifying on behalf of National Association of Convenience Stores	33
Art Potash, CEO, Potash Markets, Chicago, IL, testifying on behalf of the Food Marketing Institute	40
Ed Mierzewski, Consumer Program Director and Senior Fellow, U.S. Public Interest Research Group, Washington, DC	46

Questions for the Record:

None.

Answers for the Record:

None.

Additional Material for the Record:

American Bankers Association (ABA), Consumer Bankers Association (CBA), Credit Union National Association (CUNA), Financial Services Roundtable, Independent Community Bankers of America (ICBA), and National Association of Federal Credit Unions (NAFCU)	56
Food Marketing Institute (FMI)	59
Joint Trades Letter to HSBC	68
National Grocers Association (NGA)	71
TechNet	77

THE EMV DEADLINE AND WHAT IT MEANS FOR SMALL BUSINESSES: PART II

WEDNESDAY, OCTOBER 21, 2015

HOUSE OF REPRESENTATIVES,
COMMITTEE ON SMALL BUSINESS,
Washington, DC.

The Committee met, pursuant to call, at 11:00 a.m., in Room 2360, Rayburn House Office Building. Hon. Steve Chabot [chairman of the Committee] presiding.

Present: Representatives Chabot, Luetkemeyer, Hanna, Rice, Brat, Knight, Curbelo, Hardy, Velázquez, Hahn, Lawrence, Adams, and Moulton.

Chairman CHABOT. Good morning. I call the Committee meeting to order.

At the Small Business Committee, we make it our job to understand what is helping and hurting the small businesses that employ half of the American workforce. Today, we are interested in hearing more about the transition to EMV chip card technology because it impacts every person who holds a major credit card and the more than 20 million small businesses that accept them. So how is this transition going?

At this time last year, one credit card provider had 55,000 merchants who could accept chip cards. Now that number has grown to nearly 400,000 merchants, so we are seeing some progress. But that is still a small percentage of the small businesses in this country. One of the justifications for this shift in technology is avid security. The debate over how we secure the billions of dollars in electronic transactions that American's complete every day is not static. It requires that we continue to innovate and continue to think strategically about how we protect ourselves.

New technologies hold great promise, but there are no silver bullets, and that is why this Committee supports innovation in the electronic payments space, and we hope that small businesses will look at new securities as opportunities for better customer service. We are in the midst of a private sector transition, not something mandated by Congress or by the Administration, but something initiated by the free market. Any change is hard, but when it impacts millions of people, controversy is inevitable. That is probably the reason the Small Business Committee's hearings on the EMV transition are the first of their kind in this Congress and why we have had tremendous pushback from all sides. To me, this only confirms that this is the right issue, the right time, and the right venue for a fair, open conversation.

Let me be very clear here. We are here to examine an issue that impacts every American family with a credit card. We are not here to take sides. To better understand this transition, we need to speak to all those involved—bankers and merchants—and that is the conversation that we continue today. Two weeks ago we heard from the banks. Today, we are hearing from the merchants.

So with that I want to thank all the witnesses that have gathered here today. I would ask unanimous consent to allow one additional witness to this morning's panel. And without objection, so ordered.

And I would now like to yield to our ranking member this morning, Nydia Velázquez, for her opening statement.

Ms. VELÁZQUEZ. Thank you, Mr. Chairman.

In the last 15 years, new technologies have revolutionized the payment system, allowing customers to easily purchase goods and services and small businesses to process transactions in a quick manner. During the same period, card payments rose from 23 percent to nearly 50 percent, while payment by cash and checks dropped from 70 percent to 35 percent. This has had a significant impact on how small businesses process payments.

This trend, however, has not come without challenges. As we discussed during the first hearing on this issue two weeks ago, payment fraud has become a serious problem, not just for banks but also for companies of all sizes, including small businesses. Last year, it was reported that more than 60 percent of companies were the target of payment fraud. Globally, the United States has 25 percent of the world's credit card use, but 50 percent of the world's credit card fraud, costing more than \$5 billion. Clearly, something needs to be done to address this issue.

EMV cards are one answer. They offer a significantly higher level of data security than stripe cards. Data on the chip is secured using both hardware and software security measures, so even if the card data is compromised, the chip itself will still be difficult to counterfeit. We know that EMV is a technology that has shown great promise for reducing fraud. Much of the rest of the world—Europe, Canada, Latin America, and the Asian-Pacific region are already in the process of transitioning to EMV-enabled cards. The U.S. is the last major country to implement what is now a de facto global standard.

We are concerned, however, that small businesses remain in the dark on this transition. Most will need to upgrade their payment systems as only about 20 percent of payment terminals are currently equipped to accept chip cards, and most of these are at larger retailers. We have also heard much about the high cost of these new terminals, but I was glad to learn at the prior hearing that Square is able to provide an EMV device for as little as \$49. This should bring EMV compliance within the reach of most retailers.

Perhaps the biggest concern is the liability shift resulting from not installing the new EMV readers. Many small businesses are unaware of this new outcome, and that is the problem. Educational efforts must continue, and again, I am hopeful that more low-cost readers become readily available. However, it is also important to note that EMV is not a mandate, and businesses are not required

to install the readers if they determine that their risk of fraud is law and the transition cost is too high for them to bear.

Two weeks ago we heard from a panel of financial institutions about the rationale for this new technology and how it has the potential to reduce fraud. Today, we will hear about the experiences of those on the frontlines—small businesses—that will be using this new equipment in their stores.

I have to say that this topic has brought back memories of the interchange fee debate which this committee followed very closely. However, while both involved payment issues, my view is that they are very, very different. This current issue concerns the adoption of globally accepted fraud-prevention technology and the potential burden on small businesses. The interchange debate surrounded the transparency or lack thereof regarding the fees charged by payment network providers to merchants. I recognize the tension between these networks and those that use them, but I hope that we can focus solely on the EMV implementation issue at hand today.

With that in mind, hearings such as this present the committee with an opportunity to become a resource and sounding board for advances in finTech and payments innovation in general. The Small Business Committee is uniquely positioned at the intersection of finance and small business—the frontier really—for the adoption of these new technologies.

I thank the chairman for his leadership on this issue, and I look forward to hearing the testimony of today's witnesses. Thank you so much for taking time to be here. Welcome.

Chairman CHABOT. I thank the ranking member. And if Committee members have opening statements, we would ask that they submit them for the record.

And I will take just a moment to explain our lighting system and our rules here. You get five minutes to testify and we will have five minutes to ask questions. We will alternate back and forth, Republicans and Democrats. The green light will be on for four minutes, the yellow light will come on to let you know that you have one minute to wrap up, and then the red light means stop. And we would ask that you try to stay within that, if at all possible. We will give you a little leeway but not a whole lot.

So, and I would now like to yield to the vice chairman of the Committee, Mr. Luetkemeyer, from Missouri, to introduce our first witness this morning.

Mr. LUETKEMEYER. Thank you, Mr. Chairman. I would like to introduce a constituent of mine, Jami Wade, who is a small business owner from Jefferson City, Missouri. Five years ago she decided to follow the American dream and opened her own small business, Capitol City CORK and Provisions, a wine shop and restaurant located in historic downtown Jefferson City. In addition, Jami is executive director of Capitol City Cinema, a single screen, nonprofit community-based, member-supported movie theater. As owner and operator of two small businesses, she knows firsthand the day-to-day challenges faced by our nation's small businesses.

I want to thank Ms. Wade for taking time out of her busy schedule to be here for us today to testify on her experience with upgrading her payment card terminals to EMV technology and what this transition means as far as business. Thank you, Jami.

Ms. WADE. Thank you, Representative Luetkemeyer.

Chairman CHABOT. We will go ahead and introduce the rest of the members before we start with your testimony.

Ms. WADE. Okay.

Chairman CHABOT. Our next witness will be Keith Lipert. Mr. Lipert owns the Keith Lipert Gallery in Washington, DC, a retail establishment offering fine art and jewelry. Mr. Lipert serves on the board of directors for the National Retail Federation, and we welcome you here this morning.

Our next witness will be Jared Scheeler, who is managing director at The Hub Convenience Stores in Dickinson, North Dakota. Mr. Scheeler is a veteran of the convenience store industry and serves on the board of directors for the National Association of Convenience Stores, and we welcome you here as well.

Our fourth witness this morning is Art Potash. He is the CEO of Chicago, Illinois', Potash Markets, a small chain of neighborhood groceries in Chicago's North area. Mr. Potash is testifying on behalf of the Food Marketing Institute. We welcome you here this morning.

I would now like to yield to Ms. Velázquez for introduction of our next witness.

Ms. VELAZQUEZ. Thank you, Mr. Chairman. It is my pleasure to introduce our witness, Mr. Ed Mierzwinski, the Consumer Program Director and Senior Fellow of the U.S. Public Interest Group. With over 25 years of experience, he has testified before Congress, state legislatures, and federal agencies on a wide range of consumer issues. He has published articles in the American Prospect, the Journal of Consumer Affairs, Suffolk University Law Review, and authored the consumer reference guide "Watchdogs and Whistleblowers". Mr. Mierzwinski is also chair of the Americans for Financial Reform CFPB Taskforce. He earned both bachelor's and master's degrees from the University of Connecticut. Thank you for being here.

Chairman CHABOT. Thank you very much.

And Ms. Wade, you are recognized for five minutes.

STATEMENTS OF JAMI WADE, OWNER, CAPITOL CITY CORK AND PROVISIONS AND CAPITOL CITY CINEMA; KEITH LIPERT, OWNER, KEITH LIPERT GALLERY; JARED SCHEELER, MANAGING DIRECTOR, THE HUB CONVENIENCE STORES, INC.; ART POTASH, CEO, POTASH MARKETS; ED MIERZWINSKI, CONSUMER PROGRAM DIRECTOR AND SENIOR FELLOW, U.S. PUBLIC INTEREST RESEARCH GROUP

STATEMENT OF JAMI WADE

Ms. WADE. Good morning, Mr. Chairman, Ranking Member Velázquez, and other Committee members. My name is Jami Wade, and I am the owner of Capitol City CORK and Provisions, a wine shop and restaurant in historic downtown Jefferson City, Missouri, just a few blocks away from our Missouri State Capitol. I am also the executive director of the Capitol City Cinema.

I would like to thank the Committee for the opportunity to speak today about the matter of small businesses upgrading their pay-

ment card terminals so that those terminals can now read the new chip-enabled payment cards.

I began my adult life as a high school teacher in Columbia, Missouri. Five years ago, I moved from Columbia to my hometown of Jefferson City and opened Capitol City CORK and Provisions. I have five employees at that restaurant. We can only seat 32 patrons at our tables, so we truly are a small business. Next door to Capitol City CORK is the Capitol City Cinema, a single screen movie theater. It is a nonprofit, community-based, member-supported movie theater.

As the owner of one small business and the founder of another, I have to rely on myself to exercise sound business judgment. Any misstep could have serious consequences for the businesses I run and the people I employ. The manner in which we get paid is essential to our ability to generate cash flow, pay bills, and stay in business. Acceptance of payment cards is the lifeblood of our operations. First of all, approximately 90 percent of the restaurant sales are made through debit or credit card transactions. When a customer pays with a card, I always know I am going to get paid, get paid quickly, and get paid without hassle. My restaurant has never even had to deal with a disputed card transaction. Also, it may just be the result of basic human nature, but it seems that customers are willing to spend a little more, maybe an extra glass of wine or dessert, when they are paying with cards instead of cash. For a small business, that is valuable.

On the other hand, we do not accept checks, other than for special events, and even then, we only accept them from well-established clients. We cannot run the risk that checks will bounce and we will not get paid, leaving us to cover the cost out of pocket.

At Capitol City Cinema, many of our customers still purchase their movie tickets with cash, but we do accept cards and we often see customers making purchases of higher priced items with cards. At both Capitol City CORK and Capitol City Cinema, we have been fortunate never to have been the victim of credit card fraud payment. I know firsthand, however, that the threat is real. A few years ago, my husband was the victim of a breach at a local grocery store in Jefferson City. His card information was stolen, and the hackers ran up \$7,000 in charges. I am glad to say that we were not held responsible for paying for those transactions because those fraudulent charges would have done serious damage to our personal finances.

Both of my business rely on card payments, particularly my restaurant, and I will tell you that it would be a very big deal for us to absorb the costs associated with even one major incident of fraud. The potential liability would be seriously detrimental to our business, especially at Capitol City CORK. This is why I have made the business decision to upgrade to terminals that can read chip-enabled payment cards at Capitol City CORK and Capitol City Cinema.

A bit of background. I am lucky to have a good relationship with my card processor, another small business located a block away from the restaurant and the movie theater. Because I talked to my processor on a regular basis, I was able to learn about the new chip-enabled terminals that were becoming available, and my proc-

essor explained to me about the liability shift well before it went into effect October 1st. The total cost for a new chip-enabled terminal at Capitol City CORK is about \$300, and yes, this is an out-of-the-ordinary expense for the restaurant, but I do not consider it to be a financial burden given the peace of mind that a new terminal will provide. I look at it as paying a small premium for an insurance policy to protect the restaurant against a potentially significant downside. I cannot imagine leaving my business vulnerable to external threats when there are reasonable steps that I can take to protect it.

I also learned that a chip-enabled card reader is available for the Capitol City Cinema for \$10. I have voiced my support for making the upgrade and the decision whether to make the purchase is currently pending before the cinema's board of directors. I do believe that it is up to each business owner to make the proper decision for his or her own business. Some small business owners will no doubt choose not to upgrade their terminals, whatever the reasons. In my opinion, they are putting their businesses on the line by leaving them susceptible to fraud in card transactions.

As I started out saying, as a small business owner, I have had to rely on myself and my own sound judgment in making my vision a reality. I will continue to do so as I look ahead and upgrading to chip-enabled technology is the right decision to ensure my business is around long into the future for my family, my employees, and my customers.

I appreciate the opportunity to share my experience with the Committee today, and I welcome any questions that you may have for me.

Chairman CHABOT. Thank you very much.

Mr. Lipert, you are recognized for five minutes.

STATEMENT OF KEITH LIPERT

Mr. LIPERT. Mr. Chairman and members of the Committee, thank you for the opportunity to testify today. My name is Keith Lipert. I am a shopkeeper with one full-time and two part-time employees. My gift store, the Keith Lipert Gallery, can be found here in Washington, DC, and online at www.keithlipert.com.

I love being a retailer and I love serving my customers. When I opened my doors in 1994, I intended to be successful by selecting beautiful items to sell and by taking care of my customers. Back then, unique merchandise and quality customer service were enough to keep customers returning to my store. Manual sales slips were enough to conduct cash and credit transactions. Today, the small retail business model is being disrupted with challenges such as online competition, evolving technologies, and especially the struggle to keep up with the ever-changing compliance standards and ever-higher credit card swipe fees.

EMV was created by the largest card companies and is imposed on retailers. This October marked the deadline when card networks effectively shifted the bank's liability for fraud onto any retailer who could not accept a chip card. It is an arbitrary date and the card brands dictated it without seriously considering its effect on millions of small businesses. For businesses like mine, the EMV transition is overwhelming and costly. I do almost everything my-

self, and I must rely on outside vendors when it comes to IT needs. Selecting the right point-of-sale, EMV-compatible system can be very confusing for small merchants. There are countless options, all with their own fine print regarding new additional fees and rules. Card fees are already amongst my highest budget items. How many more card costs can there be?

Not only is the process extremely complex, but the costs can be very high. Despite claims to the contrary, the additional cost of fully incorporating EMV compliance into my POS terminal will exceed \$1,000 to \$2,000 once training, integration, and other expenses are included. There are big delays in getting the EMV hardware, installing the software, and for many retailers, receiving the certification. I cannot obtain equipment today because, as my rep explained, it is on backorder. With tens of millions of POS terminals in our country, I cannot imagine that I am the only one in this position.

As you might expect from a system where practically all the important decisions are made unilaterally by Visa and MasterCard, the migration to EMV serves the goals of their big banks and largely leave small retailers to fend for themselves. Merchants are particularly disappointed that the banks expect retailers and other businesses to adopt these costly upgrades, but the banks will not adopt secure chip and PIN technology. Chips help protect banks from the kinds of fraud they are likely to be responsible for, but in situations where retailers bear the largest share of the risk, the new chip and signature cards do virtually nothing. In those situations, notably lost, stolen, and online fraud, PINs are the single most certain way of stopping fraud.

When I opened my store, cash and checks were very common. These forms of money cost virtually nothing. A \$100 sale netted me \$100 in revenue. The card networks have spent untold millions of dollars to convince consumers to use cards instead of cash. Today, when a customer spends that \$100 using a card, I get less than \$97. This might not sound like a big reduction to some, but over the course of a year, for my one store, it amounts to tens of thousands of dollars, on par with the healthcare costs I provide. From my perspective, the whole approach to EMV is costly, incomplete, and further enhances the monopoly power of the card interest industry at my expense. Small retailers are entirely at the mercy and whims of the big banks here. We have no say, and we have no way to use the marketplace to make our objections heard and our concerns valued. Unless the government or someone can help achieve a level playing field, we will continue to see the slow destruction of the small local merchants that provide the glue for our communities.

We need two things: secure payment technology and payments that are transparent and competitive. Instead, we are getting opaque, ever-more costly half measures from our card industry partners.

Thank you for your interest in this issue, and I look forward to your questions.

Chairman CHABOT. Thank you very much.

Mr. Scheeler, you are recognized for five minutes.

STATEMENT OF JARED SCHEELER

Mr. SCHEELER. Chairman Chabot, Ranking Member Velázquez, and members of the Committee, thank you for giving me the opportunity to testify this morning on the EMV transition. My name is Jared Scheeler and I am managing director of the Hub Convenience Stores and a board member of the National Association of Convenience Stores. The Hub has four retail outlets in North Dakota where we employ on average 12 employees per store.

The EMV transition has been very costly in both time and money for my small business. We do not have the technical support a large company often has to facilitate such a massive undertaking. It has cost more than \$134,000, approximately \$44,500 per store to install EMV equipment at just three of our four stores. At our Dickinson, North Dakota store alone, the upgrade is costing us more than \$100,000. We have installed six brand new fuel dispensers at \$17,000 a piece, and installed an instore point-of-sale card reader for \$2,000. Despite these large investments, we cannot yet receive EMV transactions in part because Exxon Mobil has not yet made their card processing network EMV compatible.

At our unbranded New England in Mott, North Dakota stores, we had older fuel dispensers which would have cost \$9,000 per dispenser to upgrade. This is a common problem for smaller and more rural locations, which often have older equipment that is more expensive to upgrade, even though the dispensers still work just fine. Rather than paying \$9,000 to upgrade 20-year-old dispensers, we elected to transfer four-year-old dispensers from another store and paid \$4,000 to upgrade and transport each of those pumps. We have installed four dispensers at the New England store and are waiting to install two at the Mott store. We also had to invest in new instore PIN pads for both locations which cost \$2,000 each.

The costs I have just described are just for hardware. There are also software costs. Our Exxon Mobil branded stores will require a software update, which is part of an annual service package that cost \$1,500 per store. Without the service package, the software upgrade costs \$1,000 on its own. Once the upgrade is complete, the stores' cash registers and credit network will be unavailable for six to eight hours during the software download. We operate our stores 24 hours per day, so this downtime, which will happen during the daytime when tech support is available, will create inconvenience and costs. In fact, we estimate that it will cost more than \$10,000 in lost sales and labor at each store during that time.

Even after the EMV transition is complete at my stores, there will be significant ongoing expenses. While I know the upgrade costs from my branded stores, the costs for my unbranded locations might be higher. I just do not know yet. According to industry estimates, ongoing maintenance and upgrade expenses are expected to be upward of \$2,240 per store per year.

Although we have installed almost all the necessary EMV hardware in our stores, none of our stores have gotten the requisite software upgrades. We need to get our terminals programmed and certified to be able to handle EMV transactions, but there is a shortage of programmers and the card networks do not have enough people to certify stores like mine. Finally, we will have to

run a system pilot and engage in significant staff training before pushing our EMV system live.

Due to these delays, despite beginning the transition process early, we will not be fully EMV operable until late summer of 2016. As a small business owner, I am also frustrated because I am investing heavily in technology that provides second-rate security. In spite of the proven security benefits of chip and PIN cards, the fact that a small business like mine could implement PIN easily, the card networks are mandating chip without PIN. Thus, despite the cost, EMV will not reduce fraud as much as it could and should. This is a serious problem because retailers already pay the price for the unsecure payment card system in the form of fraud chargebacks, high swipe fees, and more. PIN could reduce fraud costs, but the card companies are not providing it on credit cards as they have elsewhere and will not let me require PIN on debit cards.

The transition to EMV has been a costly and burdensome undertaking, and unfortunately, it does not appear that the card companies took small business concerns into consideration when they came up with their EMV transition plans.

Thank you for your time, and I look forward to answering any questions you might have.

Chairman CHABOT. Thank you very much.

Mr. Potash, you are recognized for five minutes.

STATEMENT OF ART POTASH

Mr. POTASH. Good morning, Chairman Chabot, Ranking Member Velázquez, and members of the Committee. My name is Art Potash, and I am the CEO of Potash Markets in Chicago, Illinois. My family has owned and operated grocery stores in the Chicago area for 65 years. We currently employ 140 people. I appreciate the opportunity to speak to you about steps my company has taken to migrate to EMV and the challenges that we have faced.

EMV is currently not an expressed mandate on merchants; instead, Visa, MasterCard, and other card brands announced that merchants who did not migrate to EMV by October 1, 2015, would have additional fraud costs placed upon them. This is in addition to fraud costs we already pay and interchange fees and card backs. After studying if the added costs of fraudulent cards would outweigh the cost of upgrading, we decided, like the majority of the grocery industry, to migrate our stores to EMV. In making this decision, providing the most robust security for our customers' data was our central concern.

As you can imagine, upgrading to EMV is not as easy as buying a \$49.99 Square reader. Our point-of-sale equipment is complex, providing for credit, debit, snap transactions, coupons, returns, along with a customer loyalty program, and ties into a network that requires substantial upgrades and both the front and back ends to be EMV and PCI compliant. Additionally, I rely on third-party vendors to actually perform these upgrades and interface with the other links in the chain. We rely on our merchant acquirer, in our case Worldpay, to make this happen for us.

In May of 2015, we purchased and installed all new EMV point-of-sale devices in two of our three stores at a cost of \$1,000 per

lane. For the two stores, this meant \$8,000 just to conduct EMV-compliant payment transactions. This is a large investment but we were willing to make it to protect our customers. While we now have EMV-compliant readers in our stores, we are not yet EMV compliant and are facing a holiday season exposed to greater fraud liability as we wait for our merchant acquirer to complete our transition.

Currently, our acquirer estimates that they will be ready to upgrade our backend software by the end of November at best. Unlike the issuing banks who were enticed to issue chip cards with the promise of seeing their fraud costs reduced, merchants were pushed into EMV under the threat of seeing costs increase. This is particularly difficult for us to accept since we already pay the highest interchange fees in the developed world. Visa, MasterCard, and other card brands have defended charging American merchants \$71 billion a year in interchange fees as a way of offsetting the cost of fraud. In a market-based system, those fees should be reduced if fraud is reduced. Unfortunately, as we heard in the first hearing, Visa currently has no plans to pass any savings along to merchants. We hope that will change and that the Federal Reserve will see it to that it does.

Retail food companies operate at razor-thin margins due to the competitive nature of the industry. Even when food retailers have realized savings due to technological advancements, the net profits for businesses in the industry has remained below 2 percent as savings have been passed along to the customer. If retailers realize savings from reduced fraud, those savings will also be passed along to the customer.

I would be remiss if I failed to address the issue of PIN authentication. Every point of sale device in our stores is PIN-enabled. PIN is a proven safety measure that has been adopted globally but not in the United States. Historically, the card companies have ruled out EMV as chip and PIN technology, so not only are they verifying a card is legitimate; they are also confirming that the person presenting the card is authorized to use it.

Unfortunately, here in the United States the card companies have rolled out an untested model they call Chip and Choice. It is up to the issuing banks to decide whether to issue PINs. Technology and industry are evolving and improvements are made every day, but here is what we know: PIN works today. It reduces fraud, period.

In conclusion, Potash Markets has made significant investments of money and time to migrate to EMV. Unfortunately, we find ourselves waiting for our providers to get us across the finish line, while we face a busy holiday season with the threat of higher fraud liability over our heads.

I greatly appreciate the Committee's interest in this very important issue, and I look forward to answering your questions.

Chairman CHABOT. Thank you very much. Mr. Mierzwinski, you are recognized for five minutes.

STATEMENT OF ED MIERZWINSKI

Mr. MIERZWINSKI. Thank you, Mr. Chairman. Chairman Chabot, Representative Velázquez, members of the Committee, I

appreciate the opportunity to testify before you on behalf of the U.S. Public Interest Research Group. We are a coalition of non-profit, nonpartisan public interest research groups around the country that take on powerful interests on behalf of their members.

I really want to make three points in my opening statement. First, chip and PIN would have been better than chip and signature. Second, the reason that we went only to chip and signature is because the banks prefer it because they make more money. And third, a big issue before the Congress is data breach legislation. We urge the Congress not to pass any preemptive data breach legislation that takes away the right of the states to protect consumers from data breaches and other privacy and security risks.

Chip and PIN is something that has been around in Europe for over 10 years, but the United States has only been using magnetic stripe technology, which is a 1970's technology, and only recently proposed to go, as the merchants have said, to chip and signature, which prevents a card from being cloned, which prevents information from being inserted into a merchant's computer, which can be used by a bad guy to commit existing account fraud, but it does not prevent the fraud of a card being stolen and being used by an imposter. If I have your wallet with your chip card in it, I can use your chip card without a PIN, and that is the problem that we are not solving today.

Since I wrote my written testimony by the way, I found out that PIN technology also benefits merchants in online transactions, yet only one in five banks accepts online PIN debit. I am surprised that we think the fastest-growing part of fraud is going to be online fraud with the transition to chip cards, EMV technology, but why will the banks not allow the merchants to use a proven technology, PIN technologies, to prevent growing online fraud.

Well, the reason for it is quite simple. Visa and MasterCard act as a cartel. They control their payment platforms. They drive traffic to their signature-based payment platforms. That is what they want to do. The interchange fight is, I would respectively point out, related to this because in the interchange fight, we also are fighting over whether merchants can give consumers signals or the right to choose a less expensive payment method. The fight is not over the cost of interchange; it is over whether there is competition for the Visa and MasterCard controlled networks. But the fact is they control those networks. They wanted to continue and extend their dominance of those networks. That is the reason we are only going to chip and signature, which only prevents part of the fraud problem.

The October 1 switch really does not affect consumers directly. It is a business-to-business issue. As the three merchant witnesses before me have pointed out, in fact, we already have a tremendous amount of ways that the banks can collect money from merchants, and I would encourage you to ask them questions about what is the chargeback, and do you have any control over a chargeback? And do not the interchange fees already include fraud costs?

I want to point out that consumers are already well-protected by law from most existing account fraud costs. If only your bank account number or your credit card number is stolen, you are protected for 60 days on a debit card from any risk, and you are pro-

tected on a credit card from any risk of \$50 or more forever. That is why I only use credit cards. I never use debit cards. The problem with debit cards is that many consumers, they get their money back from the bank but they face the problem of cash flow, bounced checks, while they are waiting for the bank to conduct a reinvestigation. But as long as you have not lost the card, when your liability goes up dramatically with a debit card, you are in good shape if you have only lost the number.

In my remaining time I will just point out that there are many more fraud problems than existing account fraud. There is new account takeover identity theft. There is IRS tax refund fraud. There is theft of medical services fraud. And the OPM breach has demonstrated that another kind of harm that data breaches cause is reputational harm. The security clearance information that was lost by the OPM breach poses reputational risks. So I urge Congress, please do not pass almost any of the data breach laws before Congress that would narrowly protect consumers and broadly preempt the states from data security protections.

Thank you very much.

Chairman CHABOT. Thank you very much.

Members now will have five minutes to ask questions, and I will yield myself five minutes to do that.

Ms. Wade, I will start with you. What efforts have you seen made by the financial service providers to inform small businesses like yours of the EMV technology migration and the resulting liability shift? Have those efforts been helpful? Are there any things that you think should be added or changed in any way?

Ms. WADE. Sure. You know, I have the luxury of seeing my card processor once a week. He has dinner with his wife in my restaurant every Tuesday night, so I have a really personal relationship with him. And so this is a conversation we started having this summer. I was aware that it was coming. I have total faith in him, and I know that when we go live, and we have not. I have the chip reader. It goes live in a week with this particular company. I have faith that it will happen seamlessly and it will not interrupt my business.

Chairman CHABOT. Okay. Thank you very much.

Ms. WADE. You are welcome.

Chairman CHABOT. And the next one I would like to address to the three middle witnesses here. One of the things we heard at the last hearing is that some of the small businesses are waiting for the big stores to lead the way to transition to chip cards, and some of those big box stores have done so; others have not. How is the pace of the adoption of EMV technology by the big stores affecting—and a number of you have already gone ahead with this, but those in the industry that you all are part of, what are you seeing? Are folks looking towards the big box stores or not?

Mr. Lipert, I know you are a little bit of a different type of business. In fact, let me come back to you. Let me ask these two gentlemen here that question.

Mr. Scheeler?

Mr. SCHEELER. Well, I can speak first simply because our stores technology involve what you would consider big box and also independent stores because we are branded by Exxon Mobil. So the

communication from Exxon Mobil really started many years ago. But the fact that we have both branded and unbranded stores, that has dictated that since we are required by Exxon Mobil to be EMV compatible, we elected, both from a business decision and from a moral decision of protecting our customers, that we wanted to convert all of our, even our unbranded stores as well, at the same time or as close to the same time as possible.

Chairman CHABOT. Thank you.

Before I get to Mr. Potash, I meant to ask you one follow-up question, Mr. Scheeler. Since you are branded by Exxon, you had mentioned the significant costs, and they certainly are in this. Will they pay a portion or a significant amount of that cost? How much of that would be on you versus the fairly large corporate entity that we are talking about here?

Mr. SCHEELER. Yeah, 100 percent of the costs of this upgrade are on us as the business, and none of it is supported by Exxon Mobil.

Chairman CHABOT. Okay. It is a bad deal.

Mr. SCHEELER. It is.

Chairman CHABOT. Mr. Potash, if you want to go back to the big box question that I had asked, how much reliance do you see amongst small business folks on kind of waiting until those folks decide which way they are going to go on this? Is that having much of an impact?

Mr. SCHEELER. We were not waiting for the big box stores at all. In fact, we were trying to keep up with the big box stores. We wanted to be at the same level they were for protection purposes. My concern is that the fraud activity will move from the big box stores to the smaller retailers. You know, the weakest link. So the liability looms even larger than it did before. We knew about this well in advance. We bought the card readers back in May. We wanted to be ahead of the curve, and the backup system, with the rest of the links in the chain there, we are waiting on them still.

Chairman CHABOT. Thank you.

Mr. Lipert, at the hearing that we had a few weeks ago when it was mainly the banks involved, and they had argued that there was relatively low costs in a number of incidents, even down to \$49, you have obviously indicated that the costs are, in your words, overwhelming and costly. What would be your recommendation? I mean, how do you think this ought to be handled differently?

Mr. LIPERT. All of this, thank you, in terms of what to recommend, my specialty is I am a shopkeeper. I will tell you that when this came rolling in, I called my merchants. First, the provider of the equipment for what the recommendations were. They gave me a couple of options that made me a little anxious about what was going on. I was anecdotally told that some of these EMV machines were not working properly yet. I was told that at restaurants it had been a problem because the EMV technology, they were having trouble because they were certified but then they could not do tips, and so there was that. I was told that there were some problems because the transaction takes longer. And all these things made me a bit nervous. And I am a little technologically phobic anyway. So I then called my bank and I asked them to help me, to see if there was another decision. There they sent me to

somebody else. They sent me to the bank. I think in this case First State, or I had to another fellow. He told me I could buy a machine for \$600 that would go into my phone line or into a modem, but it could not work with my POS system. And the point-of-sale system is the system that allows me to know my customer history, and I have had it for 10 years, so 10 years of history, 10 years of inventory management. It sort of helps me run my business. And he said I could either use this device, the EMV device which was separate from my POSs for \$600, or he could sell me another POS system, but that system would not be compatible with my existing POS system so I would lose 10 years' worth of information. My merchant provider had said to me that whatever you do, do not go back to the side thing because it is going back to the dark ages because now you will have taken the customer staff, the inventory staff away from the payment staff and I would have to do it manually. And so that was a step backwards for me.

So I hope I have answered your question. It has been a bit overwhelming.

Chairman CHABOT. And I can certainly relate to being, I think you said technologically phobic.

Mr. POTASH. It makes me very nervous.

Chairman CHABOT. I certainly feel that way myself very often. But I will now yield to the ranking member for her time.

Ms. VELAZQUEZ. Thank you.

Mr. Lipert, can you explain why you, as a retailer, are more likely to bear the loss in a chip and signature transaction?

Mr. LIPERT. Can you repeat that to me?

Ms. VELAZQUEZ. Can you explain why you, as a retailer, are more likely to bear the loss in a chip and signature transaction?

Mr. LIPERT. Well, at the moment, when someone comes in with a fraudulent card, if it is EMV enabled and I put it into the machine, it will go through. So the signature does not really protect, as I understand it, who that person is in front of me. I just know that the card is real. In chip and PIN, I know that both the card is legitimate, and when they put the PIN that the person is legitimate. And I think that the problem with the system at the moment is we divided that. So I am more liable without the PIN.

Ms. VELAZQUEZ. Is there a way to better verify the signature?

Mr. LIPERT. We must ask for their driver's license or other forms of identification.

Ms. VELAZQUEZ. And that might require additional training to the employees.

Mr. LIPERT. Well, it is me. It is me and one other person.

Ms. VELAZQUEZ. What about a store that has more than one?

Mr. LIPERT. It is more than one. Yes.

Ms. VELAZQUEZ. Mr. Mierzwinski, you noted that Congress has occasionally examined legislative solutions to our nation's data breach program. However, one criticism of such efforts is the cost on small businesses where fraud is unlikely to reach the magnitude of those breaches suffered by the big box stores. In your opinion, what should small businesses be doing to protect their customers' data?

Mr. MIERZWINSKI. Well, I think all businesses have a responsibility under the Gramm-Leach-Bliley Act and other legislation, and

just good common sense, to protect the information of their customers. And so I would use best available technology industry standard practices is what I would do. But the problem we face here today with this issue, the issue of chip and PIN versus chip and signature to respond to the question you asked the previous witness, is really, we went to something that was best for banks, not something that was best for everybody. So as Congress goes forward, I would recommend, try to come up with technologically neutral performance standards that push industry to do a better job without forcing anything on people.

Ms. VELAZQUEZ. Yes. We have heard in previous hearings, anecdotal stories that U.S. consumers are the ones driving the use of signature instead of PIN as a matter of convenience. Would you expect any significant consumer pushback if more banks did require PINs?

Mr. MIERZWINSKI. Not at all. And by the way, we know of at least two banks, Target Bank and First Niagara Bank in Upstate New York, that are requiring chip and PIN. And also, the Federal Government, in all its cards, is requiring chip and PIN under an executive order by the president. I do not think consumers will push back. If merchants were allowed to tell them more, to signal to them more that it costs them more to pay for fraud on a signature-based platform than on a PIN-based platform, the consumers would not push back.

Ms. VELAZQUEZ. Any comments from the other witnesses?

Mr. SCHEELER. I can add to that, Ranking Member Velázquez. We deal with hundreds of card-based transactions per day in our industry, and I can say from experience that a PIN-based transaction takes no more time than a signature-based transaction. In fact, I would argue that it is actually a little bit quicker.

In addition to that, our argument for PIN, you know, I carry a debit card. I would imagine most people in this room carry a debit card that carries a PIN with it, and any time that we walk up to an ATM, ATMs that are invented by the banks using cards invented by the banks, most of them owned and operated by banks, every single time we have to utilize a PIN. If they are requiring that, there must be something to that. And I think us as retailers should have that option as well.

Ms. VELAZQUEZ. Thank you. Thank you, Mr. Chairman.

Chairman CHABOT. Thank you. The gentlelady yields back.

The gentleman from Missouri, Mr. Luetkemeyer, who is the vice chairman of this Committee, is recognized for five minutes.

Mr. LUETKEMEYER. Thank you, Mr. Chairman.

Ms. Wade, I was curious. We had a little different cost here and I want to get to Mr. Scheeler in a minute and find out what the reason was for his cost. But you indicated in your testimony that it cost you about 300 bucks?

Ms. WADE. Right.

Mr. LUETKEMEYER. It is a one-time cost; is that correct?

Ms. WADE. It is.

Mr. LUETKEMEYER. So in other words, how often do you change software on your computers or even buy a different computer to be able to maintain the kind of records you need and the

interaction with other merchants and all of your other filings that you have to do?

Ms. WADE. Okay. So I have been in business close to five years. I started out with a national processing server. I used them for two years and then I became familiar with a local processing server. So in the five years that I have been in business, I have switched one time, and it is because my local processing server offers incredible customer support and I have a personal relationship with him.

So I look at this fee, I mean, technology becomes antiquated pretty quickly. I do not assume that I will not in the future—I am going to keep up with technology—have to update again. I am prepared to do that. It is sort of like when the iPhone comes out; I like to have the newest one. I like to be up on technology. I embrace it. I think it is part of doing business and it is something that I understand and I am committed to doing.

Mr. LUETKEMEYER. You know, you made a comment a minute ago in your testimony that you do not take checks.

Ms. WADE. I do not.

Mr. LUETKEMEYER. Unless it is from a very well-established customer. So in other words, you do not have a wall behind the cashier there with all your checks pasted on the wall—

Ms. WADE. No.

Mr. LUETKEMEYER.—pasted on the wall there so people can see the folks who are kind of the stinkers in your community that you have got to be careful of?

Ms. WADE. Right. No, I do not have the wallpaper check wall behind my cash register. That is a little antiquated, too.

Mr. LUETKEMEYER. So the convenience and safety of the cards make it something—you are willing to pay the cost for the convenience and safety?

Ms. WADE. I am. I look at it as an insurance policy for my business and I look at it as one for my customers. I live in a community where most of my customers are a little older, and I think that they also value that.

Mr. LUETKEMEYER. And to me, you know, it is interesting, you know, if we knew that there were—if you knew in the neighborhood, for instance, that there were a lot of burglaries going on, you would be willing to spend some money probably to put a burglar system in to keep your business safe. Would you not?

Ms. WADE. Absolutely.

Mr. LUETKEMEYER. This kind of, I would think, would be equated to that. That is a way to keep your money safe, your transactions safe, and minimize the fraud that can happen.

Ms. WADE. Yeah. I really believe it is the cost of doing business, and I am a very tiny business. Probably the smallest one of everyone up here on this panel. And I choose that. And it is just, for me it is the cost of doing business, and I look at it as another insurance policy, and I am so insured. I am probably over insured. But that is piece of mind for me, and I think that that is important for my customers.

Mr. LUETKEMEYER. Thank you for being here, and I appreciate your entrepreneurial spirit.

Ms. WADE. Thank you.

Mr. LUETKEMEYER. Mr. Scheeler, you talked about the cost of your system, which is significantly different. I assume it is probably from the standpoint that as the kind of business that you are in, the transactions that you take at the pump are more complicated perhaps than what they are at Ms. Wade's restaurant? Or are they not? What is your costs? I am trying to make sure I understand the difference here.

Mr. SCHEELER. Absolutely. And that is a terrific question, Congressman Luetkemeyer.

I wish our system was as simplified as Ms. Wade's. However, in our industry, what we deal with is, first of all, we deal with transactions inside and outside the store. At our largest location, we have 21 different fueling stations, all which have their own independent card readers, which is a piece of hardware in and of themselves.

Mr. LUETKEMEYER. Excuse me. What does that card reader cost for each one of those different—

Mr. SCHEELER. Each individual reader is about \$1,500 each, or \$2,000—\$3,000, I am sorry, per dispenser, because they include both sides of the dispenser. So about \$3,000.

Mr. LUETKEMEYER. Why is it so much more expensive for that? Just the type of transaction that you are involved in?

Mr. SCHEELER. Certainly. The network that we are on, it is a fully integrated network that connects our fuel dispensers, our cash registers and point-of-sale system, our back office system, our scanners, and of course, our instore card readers. So the IT that goes along with that, and we are talking hardware and installation, is pretty extensive.

Mr. LUETKEMEYER. Okay. One thing that all three of you gentlemen have talked about is that you prefer to see the PIN incorporated into this as well. Is the equipment that you are installing, is it going to be able to read the PIN as well right now?

Mr. SCHEELER. I can speak for myself and my industry. I know that every card reader in my businesses have the ability, and always have had the ability to accept PIN.

Mr. LUETKEMEYER. Because I can tell you just from the testimony we had the other day, you know, the card companies are in the process of—this is a step-by-step process. Over the next 10 to 15 years, we are going to go from this to PINs, to some sort of biometric type of thing where you put your thumbprint on it or eye scan or whatever. I mean, they are going even further here. So, I mean, this is going to continue to evolve to where it gets more and more safe all the time.

But I see my time has run out, but I again thank you for your comments.

Chairman CHABOT. The gentleman yields back.

Would the gentlelady from California yield for a moment so I can ask a quick question?

Ms. HAHN. Yes.

Chairman CHABOT. I thank the gentlelady for yielding.

Mr. Scheeler, in the gas distribution business, your industry gets an additional two years, I believe, to implement all this. Is that correct?

Mr. SCHEELER. The additional time involves pay-at-the-pump. So there is some additional time that we get to get that converted, whereas our instore is in line with everybody else.

Chairman CHABOT. Okay. Thank you very much.

The gentlelady from California, Ms. Hahn, is recognized for five minutes. Thank you for yielding.

Ms. HAHN. You are the chairman. What am I going to do? Of course I am going to yield to you. I may be new around here but I know the rules.

Thank you, Mr. Chairman, Ranking Member, for holding this hearing.

As you have heard, we had another hearing a couple weeks ago and sort of heard a different story. We heard from the banks. We heard from Visa, who sort of painted a little bit of a different picture about what this process actually involved, particularly when it came to small businesses. So it is great that we are hearing from the small businesses this morning.

I conducted an informal survey with the small businesses in my community and just sort of asked them did they know, did they understand when October 1st came that that really was a pretty significant date in terms of the liability for fraud being 100 percent shifted to small businesses if they did not have this chip technology. So I found the majority of them really did not understand that October 1st date. And, in fact, I then held a small business seminar with Hispanic business owners who I found that level of knowledge was even lower in terms of their understanding. And many of them, English was not their first language, so I did not really think these banks did a good job. I mean, I think Visa told us they did a 20 city tour to roll out this new technology, which I thought was a little limited concerning how big this country is, that they only did it in 20 cities.

So I was going to ask Mr. Lipert, you know, and maybe if the other of you want to answer it, except for Ms. Wade who has dinner every week with her bank. That is sort of an unfair advantage. How was the process when you actually understood this October 1st deadline, and do you feel like it was—and I know you speak for the National Federation of Retailers—do you feel like there was a good sense, particularly maybe for business owners who had some language barriers, on the rollout of this new technology?

Mr. LIPERT. My experience was that from my involvement with my trade association, I was aware. And that did give me a leg up in starting the process of asking the questions of both my equipment supplier and then my bank. The responses I got from both really made me more nervous about the whole business, which sort of slightly froze me to put off this. In my store, I care very much about fraud and about my customers. I am a small store and I know my customers, so I think I am going to go the route of EMV and put into right all the things that are necessary, but I would like to feel that what I am doing is really going to help. And part of the problem is, as I experience it in the shop, someone coming in with a fraudulent card, it is still going to pass through the system anyway. I am not going to be able to prevent that aspect of it. If they got a proper EMV and I got the machine, it puts in, it goes through. If it is fraudulent, it is not going to make a dif-

ference. It is going to go through. So I want to make sure that I do the right thing for my customers. I try to do the right thing for myself, and try and sort out, you know, what is the right technology. And there are so many different technologies coming at me at the moment.

Ms. HAHN. Right. Right. Well, thank you.

I know I only have 50 seconds left, but I am going to move to Mr. Mierzwinski. And you all have been talking about the chip-PIN, chip-signature, and it seems like the chip signature, while maybe less secure, seems to earn more money for the banks. Could you elaborate a little bit more exactly what is the difference of the fees that the bank may earn for the signature versus the PIN?

Mr. MIERZWINSKI. Well, very quickly, Congresswoman, Visa and MasterCard own the signature networks that they try to drive all traffic to. Some of the PIN networks are owned by them but there are choices that merchants can select to have PIN networks owned by others that have lower swipe fees. That is really it in a nutshell. Visa and MasterCard have market power so they have very high swipe fees on their network which they trick consumers into using.

Ms. HAHN. And is that an impact on the consumers?

Mr. MIERZWINSKI. Absolutely. Consumers pay more at the store and more at the pump because the merchants are forced to bake these higher costs into their prices.

Ms. HAHN. Good information. Thank you.

Chairman CHABOT. Thank you. The gentlelady's time has expired.

The gentleman from South Carolina, Mr. Rice, who is the chairman of the Subcommittee on Economic Growth, Tax, and Capital Access is recognized for five minutes.

Mr. RICE. Thank you, Mr. Chairman. And I am sorry, I cannot read your nametag down on the very end there. Yes, sir. Can you tell me, you know, I understand from my old law school commercial paper about banks' liability for checks and they are supposed to recognize the signature and credit cards, and a little bit about debit cards. But can you explain for me, because you sound pretty knowledgeable about it, about online banking? Let us take it beyond the scope of this hearing a little bit. If you do online banking and you get on and you transfer money around, where does the liability lie there?

Mr. MIERZWINSKI. Congressman, in the interest of full disclosure, I am not a lawyer, although I do play one on television, but I have been working in this field for quite some time. Most transactions that are electronic are covered under the Electronic Fund Transfer Act. So your direct deposit of your paycheck and your use of debit cards and ATM cards is covered by that law. That law has a completely different fraud and liability standard than the Truth in Lending Act which covers credit cards. But when you are talking about online banking, you may also be getting into Uniform Commercial Code and other issues. But I think the big issue here today, the big question here today is in addition to the laws, you have the Visa and MasterCard rules. And in one of Congresswoman Hahn's questions, I believe she talked about the merchants not really understanding the rules or being told about the rules, and that has

been a common problem in this space. So online banking, as opposed to online retail, it is all changing.

Mr. RICE. Well, if a merchant accepts a fraudulent card under the old rules, before chip technology, magnetic stripe, who bears the responsibility for that?

Mr. MIERZWINSKI. Well, it depends on whether the merchant was in compliance with what are known as the PCI (payment card industry) standards.

Mr. RICE. Assuming that they were.

Mr. MIERZWINSKI. Did the merchant check on the back—if it is an online merchant, for example, did the merchant comply with the requirement that they check the three-digit code on the back of the card, which is something that is typically not transferred when only the front of a card or card information is swiped. If it is a gas station, did the merchant do things like ask you for your zip code or some of the other requirements? So it all depends on the rules and whether the rules were filed. Some of the merchant witnesses may have more to add on it.

Mr. RICE. But if they did comply with those rules, who bears the responsibility?

Mr. MIERZWINSKI. Well, generally, that is something that I cannot answer because I am neither a merchant, nor a bank, but I can tell you that the merchants and the banks have argued about this in court, they have argued about this in Congress, and the banks have this tremendous hammer, Congressman, what is called the chargeback. They do not get paid for their electronic transactions until the bank decides to pay them. They can keep the money through the chargeback process or they can even take it back later.

Mr. RICE. I thought under the law that, assuming that the merchants undertook their due diligence, that the credit card issuer was ultimately responsible.

Mr. MIERZWINSKI. But if you are a small 7-Eleven or a small convenience store and the bank takes your money and says it is your fault.

Mr. RICE. You are saying that may not be practical?

Mr. MIERZWINSKI. It is not practical.

Mr. RICE. Even though it is the law?

Mr. MIERZWINSKI. That is my understanding of the way it works.

Mr. RICE. Anybody up there want to add anything to that?

Mr. SCHEELER. I can add that I have heard the term “liability shift” thrown out with this EMV transition, and that has always confused me because I see chargebacks at every one of my stores, every month, of every year, that I am responsible for. The most recent one that I dealt with, I was sent the transaction information after it was disputed by whomever, by the cardholder, of the day and time and the amount of that transaction, with instructions on what the card network needed. I followed exactly what they needed. I found the actual signed slip that the customer signed, sent it in, following instructions, and I got a letter back in the mail that said, “We cannot verify this transaction.” So we did not get paid on it. So liability shift, I do not understand it because in my mind we have been liable this whole time.

Mr. RICE. Well, I think under the law, that you are not liable. Now, practically collecting that, I am not sure. And I think if you were liable for fraudulent cards and that was a widespread practice, I do not believe too many people would take the credit cards. I think that is one of the incentives to take them.

But anyway, I yield back.

Chairman CHABOT. Thank you. The gentleman's time has expired.

If I could take the prerogative of the chairman, how much of the transaction for that was in dispute?

Mr. SCHEELER. It was either \$46 or \$56. I do not remember the exact amount.

Chairman CHABOT. Okay. Thank you.

The gentlelady from Michigan, Ms. Lawrence, is recognized for five minutes.

Ms. LAWRENCE. Thank you.

Mr. Lipert and Mr. Scheeler, you both represent the National Retail Federation Convenience Store Association where you are small business owners. So let us be clear. There seems to be less of an urgency for smaller businesses that handle low volume or you know your customers, like Ms. Wade has said. It is a smaller community, so you know your customers basically when they come in. How can we encourage small business owners to make this transition? How do we make the case that the challenges that a small business owner are faced with during this process is worth it? Can the two of you please comment on that?

Mr. SCHEELER. I think that is a terrific question. I think depending on the volume of the store, economically, there is a legitimate question over whether the upgrades should take place or not. I think what really should be the deciding factor for any legitimate businessperson is, do I have a moral responsibility to my customers? Do I want them to feel comfortable processing their payment cards in my place of business? And I think most businesses would say, "Yes, absolutely I do." So I think speaking for just ourselves and our smaller stores, that was a deciding factor when I was making the decision to transfer to EMV.

Ms. LAWRENCE. I did not really get an answer before. At least I did not hear it. What is the cost that you say if you average it out for small businesses to be able to have the equipment and to transfer to this new technology?

Mr. SCHEELER. Okay. And again, it is going to be different for my industry as opposed to others. The industry average in the convenience store industry is about \$26,000 per store because there are so many different moving parts involved. As I said in my testimony, it was about \$44,000 per store because there were some other considerations involved as well. So the bottom line is the numbers are pretty significant.

Ms. LAWRENCE. Okay. Mr. Scheeler? That is you. So, Mr. Lipert?

Mr. LIPERT. I think for small stores like myself, I think if we could be provided secure payment technology and payments that are transparent and competitive, this would be really helpful.

Ms. LAWRENCE. Absolutely. We want to protect our customers. We care about our customers. When I started my testimony, I am

a shopkeeper because I love my stuff and I love my customers. I want to do the best for them and give them the best service and experience.

One thing I would just like to add is that in terms of this cost, I was given an option of doing an EMV reader. So that is the actual little boxy thing that plugs into a model or into a phone line that can take a payment. That I was quoted \$600 for. The problem for small businesses, shops that have stuff, shops where there is inventory, shops where there are customers that are repeating and coming in, in order to just stay current, we have to have a point-of-sale system, and the point-of-sale system is the thing that sort of links my stuff to my customers so that I can look back and see who bought what, did what, and all the rest of it. And it is connected also to the payment. Once you get into that, it becomes very expensive, and this is the problem, and this is what is causing me such reluctance. Yes, I could go and buy the box, but as my equipment provider said to me, "Do not do that, Keith. That is going back to the Dark Ages." So that is my dilemma. Yes, I can buy the box for \$600 and satisfy a minimum requirement, but it does not help me try and keep my business current and competitive with all the other stuff that is going on in our industry.

Ms. LAWRENCE. Thank you for that.

Just briefly, Mr. Mierzwinski, in your testimony, you highlighted that the Federal Trade Commission noted that the EMV rollout and the October 1st deadline is being taken advantage of by scam artists. Can you elaborate on that?

Mr. MIERZWINSKI. Well, certainly, Congresswoman. The scam artists come out every time there is a new way that they can hook an old scam up to it. And in this case, consumers are getting letters that claim to be from their bank that are trying to obtain information. They say, "You have not gotten your chip card yet. You are in trouble. We are going to send it to you but first you need to verify your current account number." They trick you, social engineering, into giving them information that allows them to rip you off.

I would point out that I think, I am speculating here, that I am sure there are also similar scams directed at the merchants, trying to get them to buy weak technology or overpriced technology that will not work. That typically happens as well, small business fraud.

Chairman CHABOT. The gentlelady's time is expired.

Ms. LAWRENCE. Thank you.

Chairman CHABOT. Thank you.

The gentleman from Nevada, Mr. Hardy, who is chairman of the Subcommittee on Investigations, Oversight, and Regulations is recognized for five minutes.

Mr. HARDY. Thank you, Mr. Chairman.

In the wake of this change and during this process we have seen a lot of fraud going on, and also the businesses having the opportunity to change. Are there certain levels or categories we find through the fraud process that if you have certain information you can categorize your information that can be breached through this process? This would probably be best for you, Mr. Mierzwinski. Are there levels that businesses can take of this or is it open, you know, my data, I do not want all my information out there, but

when you have a credit card and you file for it, you pretty much give the bank all your information. Does that liability fall back on these small businesses when all that liability is reached? Or are there certain levels you businesses have that you can only acquire? Does it make sense what I am trying to ask there?

Mr. MIERZWINSKI. Well, I think, Congressman, you have asked a couple of questions. But going to EMV or chip cards is going to prevent merchant computers from getting your credit card or debit card number inserted into them. It basically makes every transaction establish a one-use number based on that transaction. So the big breaches with thousands of cards being cloned will no longer occur from chip cards, but there will still be fraud by imposters, and there will still be bad guys digging into computers systems to obtain the other kinds of information that allows them to also commit new account identity theft, or in the case of the IRS, steal your tax refund, et cetera. So I would leave it to the merchants. The merchants have an issue with the banks. As of October 1st they are saying if you have not installed readers for chip cards, you will be more liable, but as the merchants have already pointed out, we are already liable.

Mr. HARDY. I guess this is for all the merchants. The question I would have is it sounds like a cost for each one of you, where does that cost get handed down to? We know where it goes but I do not think you take it on yourself. Does that get passed on to the consumer, these changes? And is it exponentially higher for certain businesses and lower for other bigger businesses? Does anybody care to address that?

Mr. SCHEELER. I would, Mr. Congressman. Thank you.

I think the free market would dictate that typically those costs would get passed on to consumers. In my industry though, I see it differently simply because our primary product in the convenience store industry is gasoline. We are the only industry in the world that puts a big sign up on the corner and plasters our gas price up there for everybody to see. So if I decide to raise my price two cents, whatever it might be per gallon, the guy down the street, in true competition, may or may not do that. So market forces will drive that price in our industry, so I do not think that applies because of the transparency that we carry that quite frankly the banks do not know much about.

Mr. HARDY. This process of we are doing chip and signature now, and I know the banks have committed they are going to move towards PIN and other identification processes. Do you have any idea why they are waiting and why we did not try to implement this at the time with the technology? Mr. Mierzwinski, maybe you have that idea.

Mr. MIERZWINSKI. I think nobody can figure out any reason that the banks are delaying and slow-walking this transition except that they make more money on chip and signature than they would on chip and PIN because there would be competing networks that merchants could choose or encourage their customers to choose that are owned by different people than Visa and MasterCard. Consequently, the banks would earn less money. That is really the reason that I can see.

Mr. HARDY. Thank you, Mr. Chair. Most all my other questions have been asked prior to this, so I will yield back.

Chairman CHABOT. Thank you very much. The gentleman yields back.

And we want to thank the witnesses for their testimony here today. We have now heard a couple of weeks back from the bankers and credit card issuers on one hand, and we have heard from the retailers this week, so we have, I think, a good sense from both sides where some of the issues are and what is happening. I think you have helped educate the Committee, and hopefully through our means of communicating to the public, we will be educating the public more and more, as well, because they are, after all, going to be directly affected by this very important issue.

I would ask unanimous consent that members have five legislative days to submit statements and submitting materials for the record.

Ms. VELÁZQUEZ. Not in Washington.

Chairman CHABOT. Not in Washington. Although I have to note, I am not a frequenter of art galleries, but your shop, Mr. Lipert, sounds like it would be a fun place to go and interact and just see all the things that you have there. So it is not a commercial, but I thought your testimony was very helpful, as was all the testimony that we heard this week, as well as a couple weeks ago.

So if there is no further business to come before the Committee, we are adjourned. Thank you very much.

[Whereupon, at 12:17 p.m., the Committee was adjourned.]

A P P E N D I X**Hearing Entitled “The EMV Deadline and What it Means for Small Businesses: Part II”****Testimony of Jami Wade, Owner, Capitol City CORK and Provisions and Executive Director, Capitol City Cinema****Before the U.S. House of Representatives Committee on Small Business****October 21, 2015**

Good morning, Mr. Chairman, Ranking Member Velazquez, and other Committee Members. My name is Jami Wade, and I am the owner of Capitol City CORK and Provisions, a wine shop and restaurant in historic downtown Jefferson City, Missouri, just a few blocks from the Missouri State Capitol. I am also the executive director of the Capitol City Cinema. I would like to thank the Committee for the opportunity to speak today about the matter of small businesses upgrading their payment card terminals so that those terminals can read the new chip-enabled payment cards.

I began my adult life as a high school teacher in Columbia, Missouri. Five years ago, I moved from Columbia to my home town of Jefferson City and opened Capitol City CORK and Provisions. I have five employees at the restaurant, and we serve a seasonal and changing menu with locally sourced food. We can only seat 32 patrons at our tables, so we truly are a small business. Next door to Capitol City CORK is the Capitol City Cinema, a single-screen movie theater that specializes in showing independent, foreign, and documentary films. It is a non-profit, community-based, member-supported movie theater.

As the owner of one small business and manager of another, I have to rely on myself to exercise sound business judgment. Any misstep could have serious consequences for the businesses I run and the people I employ. The manner in which we get paid is essential to our ability to generate cash flow, pay the bills, and stay in business. Acceptance of payment cards is the life-blood of our operations. First of all, approximately 90 percent of the restaurant's sales are made through debit or credit card transactions. When a customer pays with a card, I always know I am going to get paid, get paid quickly, and get paid without hassle. My restaurant has never even had to deal with a disputed card transaction. Also, it may just be the result of basic human nature, but it seems that customers are willing to spend a little more—maybe an extra glass of wine or dessert—when they are paying with cards instead of cash. For a small business, that's valuable. On the other hand, we don't accept checks other than for special events and, even then, we only accept them from well-established clients. We cannot run the

risk that checks will bounce and we won't get paid, leaving us to come out of pocket to cover costs.

At Capitol City Cinema, many of our customers still purchase their movie tickets with cash. But, we do accept cards, and we often see customers making purchases of higher-priced items with cards. For example, they might sign up for an annual membership giving them discounted admissions and other perks throughout the year. These purchases are essential to the business, because without our member support we could not remain operational.

At both Capitol City CORK and Capitol City Cinema, we have been fortunate never to have been the victim of payment card fraud. I know first-hand, however, that the threat is real. A few years ago, my husband was the victim of a breach at a grocery store in Jefferson City. His card information was stolen, and the hackers ran up seven thousand dollars in charges. I am glad to say that we were not held responsible for paying for those transactions, because those fraudulent charges would have done serious damage to our personal finances. Both of my businesses rely on card payments, particularly my restaurant, and I will tell you that it would be a very big deal for us to absorb the costs associated with even one major incident of fraud. The potential liability would be seriously detrimental to our business, especially at Capitol City CORK. This is why I have made the business decision to upgrade to terminals that can read chip-enabled payment cards at Capitol City CORK and Capitol City Cinema.

As a bit of background, I'm lucky to have a good relationship with my processor, another small business located a block away from the restaurant and the movie theater. The processor is the company that sells and services the technology for my businesses to be able to accept card payments and get connected to a merchant acquirer. Because I talk to my processor on a regular basis, I was able to learn about the new chip-enabled terminals that were becoming available and my processor explained to me about the liability shift well before it went into effect on October 1. For now, it seems that most of the local banks and credit unions in Missouri have not issued cards with chips on them, but I understand that this is coming soon. When it happens, I want to be prepared and I want to be protected by the liability shift—this means putting in new terminals.

The total cost for a new chip-enabled terminal at Capitol City CORK is about three hundred dollars. Yes, this is an out-of-the-ordinary expense for the restaurant, but I do not consider it to be a financial burden given the peace of mind that a new terminal will provide. I look at it as paying a small premium for an insurance policy to protect the restaurant against a potentially significant downside. After having survived the first few years running my own business—a period in which many new start-ups fail—I cannot imagine leaving my business vulnerable to external threats when there are reasonable steps that I can take to protect it. Furthermore, from all of the information I've received from my processor, I expect the process to upgrade to the new terminal to go seamlessly, without any disruption to our everyday business. In

fact, we have the new terminal on site. It just hasn't "gone live" yet but should by the end of this month.

I also learned that a chip-enabled card reader is available for only fifty dollars for the Cinema. I have voiced my support for making the upgrade, and the decision whether to make the purchase is currently pending before the Cinema's board of directors.

I am a person who left her job to pursue a vision of running her own business. When I get out and talk to other members of the downtown Jefferson City community, every small business owner has a story that is unique, but most of us have in common that we accept payment cards because they are valuable to our businesses. In light of the recent headlines about several data breaches over the last few years, many other small business owners in Jefferson City and I wonder, what's to stop it from happening here? They share my concerns and want to do everything they can to protect their businesses and their employees—and I suspect that this sentiment is widespread across the country. I do believe that it is up to each business owner to make the proper decision for his or her own business. Some small business owners will no doubt choose not to upgrade their terminals, whatever the reasons. In my opinion, they are putting their businesses on the line by leaving them susceptible to fraud in card transactions. As I started out saying, as a small business owner, I have had to rely on myself and my own sound judgment in making my vision a reality. I will continue to do so as I look ahead, and upgrading to chip-enabled technology is the right decision to ensure that my business is around long into the future for my family, my employees, and my customers.

I appreciate the opportunity to share my experience with the Committee today, and I welcome any questions that you may have.



STATEMENT OF KEITH LIPERT
OF THE KEITH LIPERT GALLERY

FOR THE

COMMITTEE ON SMALL BUSINESS
OF THE
UNITED STATES HOUSE OF REPRESENTATIVES

HEARING ON
“THE EMV DEADLINE AND WHAT IT MEANS FOR SMALL
BUSINESSES PART II”

WEDNESDAY, OCTOBER 21, 2015

Keith Lipert
Keith Lipert Gallery
2922 M Street NW
Washington, DC 20007
202.965.9736

Chairman Chabot, Ranking Member Velazquez, and distinguished members of the Small Business Committee, thank you for inviting me to testify at this important hearing, “The EMV Deadline and What it Means for Small Businesses Part II.” My name is Keith Lipert and I am an independent shopkeeper. I own The Keith Lipert Gallery, and my storefront can be found right here in Washington, DC and online at keithlipert.com. I am a sole proprietor with one full-time employee and two part-time employees. I love being a retailer and I love serving my customers.

In addition to running my store, I serve on the Board of Directors at the National Retail Federation (“NRF”). NRF is the world’s largest retail trade association, representing discount and department stores; home goods and specialty stores; Main Street merchants; grocers; wholesalers; chain restaurants; and Internet retailers from the United States and more than 45 countries. Retail is the nation’s largest private sector employer, supporting one in four U.S. jobs and 42 million working Americans. Retail contributes \$2.6 trillion to annual GDP and is a daily barometer for the nation’s economy. Retailers create opportunities for life-long careers, strengthen communities, and play a critical role in driving innovation. Many of NRF’s small business members, like millions of other small merchants, are being adversely affected by the card brands concerted effort to force us to further adapt our operations to their flawed card system. I want to give you a sense of our challenges and ask for your help.

When I opened my doors in Georgetown in 1994, I intended to be a successful merchant by selecting beautiful items to sell and by taking care of my customers. In those days, unique merchandise and quality customer service were enough to keep customers returning to my store and manual sale slips were enough to conduct credit card transactions. Today, that simple business model is being disrupted with overwhelming challenges such as online competition, evolving point-of-sale systems (“POS”), and the constant struggle to keep up with ever-changing compliance standards and ever-increasing credit card interchange rates, or swipe fees. All retailers, no matter the size, are being held to technological standards that even some of the most sophisticated businesses in the world have yet to master.

EMV (the name is from the initials of the owners—Europay MasterCard Visa) is a proprietary standard that was created by the largest card companies to be imposed on retailers. U.S. banks are just now issuing updated cards with chip technology, protected by the signature authentication (“chip and signature”). Consumers around the world have been using chip cards for decades. However, in the rest of the world chip cards are accompanied by Personal Identification Numbers (“PINs”). PINs are proven to be a much more secure authentication method in transactions and, unlike Chips, effectively reduce nearly all types of fraud. In fact, according to the Federal Reserve, PIN cards are up to seven times more se-

cure than Signature cards¹. Chips help protect the physical card and PINs reliably authenticate the consumer. This combination is precisely the sort of protection that the American consumer wants now².

October 1, 2015 marked the deadline when card networks effectively shifted liability for fraud onto any retailer without the ability to accept a chip card presented to her for transaction. This so-called “deadline” of October 1st was an arbitrary date that the duopolistic bank card brands dictated without seriously considering its effect on millions of small businesses. No one from my bank processor or existing supplier even contracted me about the need to add a new EMV device, let alone a deadline by which to do so. The most shocking part of this news was that the already sky high swipe fees will stay high and are rationalized as the cost of fraud prevention, even though the liability for fraud is now being shifted to me.

The EMV transition is overwhelming and expensive for an independent, small retailer. I do not have an IT department; I personally handle IT—as well as payroll, benefits, taxes, buying, selling, and everything else a small business owner must do to say in business. I rely on service providers and vendors when it comes to IT needs through consultation over the telephone. Unfortunately, a phone conversation doesn’t cut it when it comes to adopting complicated payment technology systems. Not only is the implementation process extremely complex, but also the cost is extremely high for merchants of all types (whether retailers or restaurants or taxicabs or doctors’ offices). There are wide ranges of estimates for the cost attributed to upgrading terminals, but it is fair to say that for many businesses the costs for fully functional POS terminals that comply with EMV can easily exceed \$1,000 to \$2,000 once all of the training, system integration, and back office costs are included³. Retailers strongly support more secure payment options, and that is why we are collectively spending our share of billions of dollars to adopt the chip card technology even when it makes little sense in any serious customer protection or basic return-on-investment analysis.

But that is why we also find it extremely frustrating that the card industry expects retailers and other businesses to upgrade when it will not allow the US to adopt the most secure form of this technology—chips with PINs. Take lost-and-stolen fraud, for example, which is the kind of fraud that chips with signature alone will do nothing to prevent. The card industry maintains that lost-and-stolen fraud is declining, but a more nuanced evaluation of the data shows that lost and stolen fraud has remained largely constant while counterfeit card fraud and card-not-present (“CNP”)

¹ Board of Governors of the Federal Reserve System, “2011 Interchange Fee Revenue, Covered Issuer Costs, and Covered Issuer and Merchant Fraud Losses Related to Debit Card Transaction,” March 5, 2013, p. 25, http://www.federalreserve.gov/paymentsystems/files/debitfees_costs_2011.pdf

² Chip & PIN Security Now! Research TargetPoint Consulting, November 2014, <http://www.chipandpinsecuritynow.org/about/#sthash.c9uJZLis.dpuf>

³ Chris McWilton, President, MasterCard North America. “Credit Card Chip Gains Traction.” Squawk on the Street. CNBC, New York. <http://video.cnbc.com/gallery/?video=3000427478>

fraud have risen.⁴ The use of PINs will mitigate fraud in all of these situations. But in the two specific situations where retailers bear the largest share of the risk—and where chips do virtually nothing—lost and stolen and CNP—PINs are not just a mitigating factor to fraud, they are the single most certain way of blocking it.

In addition to the significant costs, there are significant delays in getting the POS hardware, installing the software, and, for many retailers, receiving the certification. There are tens of millions of POS terminals in our country, but small business updates are simply not a priority for the hardware manufacturers, the software service providers, nor the certification entities. I asked my payment technology rep when I could expect a new device if I ordered it this month and was told the equipment is on backorder.

The delays for the equipment to arrive in my store takes into account the assumption that I even know which system to choose in the first place; there are countless options for retailers, all accompanied by their own fine print regarding fees and rules. EMV is all new to me, and banks and the networks are not contacting small businesses to help facilitate the transition in any way. What may seem like a “deal” for an EMV reader is in fact a solution that will come with increased costs over time. Customers use many different kinds of cards, all with different interchange rates, or swipe fees. Now, will there be more fees on my statement to accept EMV dips after I install new readers? How many more fees can there be?

When I started in retailing, cash and checks were very common. Both of these forms of money cost me virtually nothing. \$100 in cash nets me \$100 in revenue. These days, however, the card networks and banks spend billions of dollars promoting the use of a more expensive form of money: cards. Now a \$100 sale might net me \$97 in revenue, because the card industry is charging *me* for *their* rewards programs. In fact, for most retailers, swipe fees are the second or third highest cost for merchants behind labor and rent.

All of this would not have happened if two companies, acting on behalf of thousands of banks, hadn’t been allowed to subject consumers and businesses to an expensive, fraud-prone payment system. From a small retailer’s perspective, the whole approach to EMV is costly, incomplete, and further enhances the monopoly power of the card industry at my expense. If banks and card networks are going to make me spend a lot of money to reduce their fraud, they should at least offer a more secure solution and a savings to me and my customers.

Small retailers are entirely at the mercy and whims of the big players. We have no say and no way to use the marketplace to make our objections heard and our concerns valued. Until the government can help effectuate a level playing field, we will continue to see the slow destruction of the local merchants that provide the glue for our communities. We need a secure payment technology so

⁴ Board of Governors of the Federal Reserve System, “2011 Interchange Fee Revenue, Covered Issuer Costs, and Covered Issuer and Merchant Fraud Losses Related to Debit Card Transactions,” March 5, 2013, p. 25, http://www.federalreserve.gov/paymentsystems/files/debitfees_costs_2011.pdf

lution that trends to processing on par with cash. Instead we get costly alternatives.

Thank you for your interest in this issue, and I look forward to your questions.

TESTIMONY OF
JARED SCHEELER
MANAGING DIRECTOR
THE HUB CONVENIENCE STORES, INC.
ON BEHALF OF
THE NATIONAL ASSOCIATION OF CONVENIENCE
STORES
FOR THE
HEARING OF THE HOUSE SMALL BUSINESS COMMITTEE
OCTOBER 21, 2015
“THE EMV DEADLINE AND WHAT IT MEANS FOR SMALL
BUSINESSES: PART II”

My name is Jared Scheeler. I am Managing Director for the Hub Convenience Stores, Inc. and I appreciate this opportunity to present my views regarding the implications of the EMV chip deadline for my small business.

I am testifying today on behalf of the National Association of Convenience Stores (NACS). I serve on the NACS Board of Directors. NACS is an international trade association representing more than 2,200 retail and 1,800 supplier company members in the convenience and petroleum retailing industry. NACS member companies do business in nearly 50 countries worldwide, with the majority of members based in the United States. In 2014, the industry employed more than two million workers and generated \$969.1 billion in total sales, representing approximately 4.0 percent of the United States' GDP—or one of every 25 dollars spent. The majority of the industry consists of small, independent operators. More than 70 percent of the industry is composed of companies that operate ten stores or fewer, and 63 percent of them operate a single store.

My company, Hub, has four retail outlets in North Dakota. Two locations are located in Dickinson, one in Mott, and one in New England, ND. On average, we employ 12 employees per store.

As a small business, the transition to EMV has been a costly and burdensome undertaking. It does not appear that the card companies took into consideration the realities of operating a small business when they came up with their transition plans. In addition to the substantial time and money involved, the card companies have erected considerable obstacles that restrict my ability to reduce payment card fraud at my stores. Below I offer more detailed comments on the transition, its impact on my business, and the lost opportunity for substantially reducing fraudulent transactions.

I. The cost of the EMV transition for my business.

Thus far, it has cost approximately \$44,500 per store—more than \$134,500 for a chain our size—to make the point-of-sale operating systems and fuel dispensers in our three existing stores EMV compatible. At our existing site in Dickinson, which is Mobil-branded, we purchased 6 brand new fuel dispensers even though the existing dispensers had many years of useful life in them. The new dispensers were \$17,000 each and the in-store point of sale card reader was \$2,000. So, the upgrade cost us more than \$100,000 at this site.

Although we made these large investments, because we process our cards at our existing and new Dickinson sites through our fuel brand, ExxonMobil, we cannot accept EMV transactions. That is because ExxonMobil has not yet implemented EMV technology in their card processing network. They are not mandating an in-store terminal switch until October 1, 2016 and they are assuming any liability between now and that date.

Once they implement the EMV technology, all ExxonMobil stores will require a software update. These updates are one part of an annual service package that cost \$1,500 per store. For those who don't purchase the service package, it's about \$1,000 for the soft-

ware upgrade alone. Further, when the upgrade occurs, the store's cash registers and credit network will be unavailable for 6–8 hours while the software download occurs. We operate our stores 24 hours per day so this downtime will inconvenience our customers and lose us money. In fact, we estimate that during the time our stores will be “offline” for the software update, we will lost at least \$10,200 in sales as well as labor and overtime costs per store.

Unlike our store in Dickinson, the New England, ND store does not carry the brand of a major oil company. This store had older dispensers that still had many useful years in them as they don't pump a large amount of fuel. There are four dispensers at this store. Upgrading these older dispensers would have cost about \$9,000 per dispenser. This is a problem for smaller and more rural locations. They often have older equipment that is more expensive to upgrade even though it may have more useful life. Rather than pay \$9,000 to upgrade 20 year old dispensers, we elected to transfer 4-year old dispensers from West Dakota Oil to this store, and we put in the new, compliant dispensers at West Dakota. The New England Store bought the 4-year old dispensers from West Dakota Oil, and paid \$3,000 to upgrade each of those pumps plus \$1,000 to transport each pump. This store also installed EMV card readers inside the store. In spite of these investments, the store cannot yet accept EMV transactions due to delays in the software programming necessary to take the transactions.

As in New England, our store in Mott, ND is unbranded. We have two dispensers left over from the West Dakota Oil that will eventually be installed here. Like the New England store, these dispensers would cost \$3,000 each to upgrade plus \$1,000 to transport each dispenser. We plan to wait to install these dispensers due to the cost to upgrade.

These costs are staggering. The average convenience store makes \$47,000 in profits in a year. That is pre-tax. Costs in the low six figures are too much for most to absorb. The average industry cost, thankfully, is lower than ours. Some of that difference is driven by the fact that we had some older equipment that needed to be replaced rather than upgraded. Again, that will hit smaller and more rural locations the hardest.

Across the industry, the average cost per store is estimated to be about \$26,000. With 152,000 stores across the United States, that means our industry will pay about \$3.9 billion to move to EMV.

And the transition is costly not only in monetary terms, but also in terms of staff time and effort. As a small business owner, I do not have the back office or technical support of a large company. I have invested a tremendous amount of my own time to effectuate this transition, at the expense of tending to other business matters.

My company began the EMV transition process in October 2014 and it took about 16 weeks just to receive the necessary hardware. We have been at this a long time and we are still not done. While hardware has been a major expense, it is only the beginning. None of our stores have gotten their necessary software upgrades—and we can only proceed with the next steps in the EMV transition process after that happens. Then, we move onto what may be the

biggest stumbling block, getting technicians to program the new equipment according to card company specifications and getting certification. Each of the major card brands—Visa, MasterCard, American Express and Discover—require separate certifications. And, we need to get separate certifications for credit, PIN debit, and signature debit. The certification process is lengthy and frequently leads to delays because the card networks have not provided the resources necessary given the large number of merchants that needed certifications by the same deadline. Getting programming and certification, however, is not the end of the EMV journey. Businesses still need to engage in pilot testing and have significant staff training in order to be able to start taking EMV transactions.

Given all this, it is not surprising that my company and other small businesses are finding this transition difficult. The timeframes have been unrealistic and the card brands have not provided the support necessary to get this done in the timeframe they themselves set. Small businesses, not surprisingly, get pushed to the back of the line to get programming and certification services that are necessary to complete these projects. Wait times are long. And, even when those wait times are done, to avoid inconveniencing customers, we often have to work at odd hours to install and program new EMV terminals.

Even after the EMV transition is complete at my stores, I have serious concerns about the ongoing expense and burden of the new system. The costs for getting those services from ExxonMobil, as noted above, are high, but at least I know what they are. The costs for my unbranded locations might be higher—I just don't know yet. In fact, according to industry estimates, on-going maintenance and upgrade expenses are expected to be upward of \$2,240 per year, per store.

II. Retailers like me already bear the brunt of an unsecure payments system

As a small business owner, I am absolutely committed to improving payment card security. I have no problem making investments in *effective* fraud-prevention measures because retailers already pay the price for the unsecure payment card system. Unfortunately, as discussed in further detail below, this very costly transition to EMV will not reduce fraud as much as it could and should, and my business will continue to suffer from a deeply flawed system.

Banks often claim that they are on the hook for fraud losses. They also claim that they provide a “payment guarantee” to their retailer customers. Frankly, I find these claims offensive because they are false. Let's be clear, I pay for fraud several times over:

First, I pre-pay for fraud with exorbitant swipe fees, which the card networks have justified as necessary to cover the cost of fraud and fraud prevention. The Federal Reserve's rules on debit card swipe fees specifically provide for merchants like me to pay 5 basis points (0.05% of the transaction amount) on every transaction to cover banks' fraud losses. That amount is now higher than the full amount of debit card fraud suffered by the majority of banks cov-

ered by the Fed's rules. And, credit card swipe fees and debit swipe fees for banks not covered by the rules are much higher—ensuring merchants pay for more than 100% of fraud up front.

Second, I pay for fraud in chargebacks. Despite banks' false claims of providing a "payment guarantee" to me and other retailers, when a fraudulent charge is made, my company is "charged back" for the amount of the fraudulent transaction about three out of four times. In fact, every year our company pays \$600 per store in chargebacks.

Third, if a merchant suffers a data breach, Visa and MasterCard rules require the merchant to pay for any increase in fraud for those breached accounts.

Overall then, merchants pay for far more than 100% of the card fraud already. Now, for those who have not yet been able to complete the changeover to EMV, the numbers will be even higher. That makes no sense.

III. EMV will not reduce fraud nearly as much as it should

Disappointingly, the card companies have mandated an EMV transition that does not include a simple and *very* effective security measure that would substantially reduce fraud losses for everyone, including small business owners like me. Instead of migrating to chip-and-PIN technology in the U.S., the card companies have opted for a transition to chip-*without*-PIN. This is true in spite of the fact that the rest of the world has been moving to chip-and-PIN and that the data the card industry has used to justify the move in the United States relies on the use of chip-and-PIN, not chip-without-PIN.

Chip-embedded cards are harder to counterfeit or copy than magnetic stripe cards, but counterfeit "chip" cards (that don't have a chip but still look like a chip card) can still be made, and when a person presents a card with a non-functioning chip, the card's magnetic stripe will be used or the card's number will be entered to complete the fraudulent transaction. Most of those transactions would, however, be blocked if a PIN was required.

Chip technology without a PIN does not help reduce fraud in instances where a card is lost or stolen. Chip-without-PIN also does not stop card fraud on the Internet. But Internet fraud is already a major proportion of fraud and will undoubtedly grow along with the EMV implementation. PIN use can help stop lost and stolen fraud as well as Internet fraud. The fact that the card industry is not issuing a PIN with every card is mind-boggling and cuts against all of the experience we have gained with the technology overseas.

This is particularly important in my business since 35 percent of our sales occur at the pump where the store clerk does not see the card user or the card for sales. Over the past few years, motor fuel and other retailers with self-serve machines have paid fees to require zip code verification for these transactions. This service adds cost but saves us real dollars on fraud chargebacks. While generic zip code verification helps, PIN authentication—which is truly indi-

vidualized for each consumer—works better. The benefits of PIN authentication are real: the Federal Reserve Board has confirmed that PIN authentication is *six times* more secure than signature authentication on debit transactions.¹ Moreover, chip and PIN has been used to great success in Europe for over twenty years—a fact the card networks know well.²

Despite the clear security benefits of PIN, the card companies continue to adopt policies and rules that do not capitalize on those benefits. The EMV transition to chip-without-PIN is just one example. Another example is the card companies' prohibition on merchants requiring PIN on debit card transactions. Even though the vast majority of debit cards are PIN-enabled, under the card companies' rules, I cannot choose to require customers to use a PIN to authenticate debit transactions. That is true in spite of the fact that when banks act as merchants—dispensing cash from ATMs—they are allowed to require PINs. And, of course, the banks always do require PINs.

The card companies' actions and policies simply do not make sense if the real objective is to reduce fraud in the payment card system. Perhaps this should not be a surprise given that those networks do not shoulder any of the losses from fraudulent transactions. But as a small business owner paying for this costly EMV transition and substantial annual fraud costs, I am frustrated that I will not see the fraud relief that I and other retailers could easily get if the networks were making the type of genuine fraud-reduction effort that they have made around the world.

IV. PIN authentication would also benefit our customers.

I have heard the card companies and banks say time and time again that American consumers do not want PIN authentication. According to them, consumers will refuse or be unable to remember a 4-digit code. Given consumers' daily usage of PINs at bank ATMs and their use of similar passwords and codes to access smart phones, other devices and online accounts among many other things, this is demonstrably wrong. And, the card industry position is not supported by the data—a recent survey commissioned by the National Retail Federation found that 62% of consumers would prefer to use chip and PIN cards rather than chip-without-PIN cards.³

The card networks' position against PIN use in the United States appears to be disingenuous given that they have advertised in other countries that PIN transactions are more effective in pre-

¹Federal Reserve Board, Debit Card Interchange Fees and Routing, 77 Fed. Reg. at 46,261 (Aug. 3, 2010), available at <http://www.gpo.gov/fdsys/pkg/FR-2012-08-03/pdf/2012-18726.pdf>.

²*The Benefits of Chip and Pin for Merchants*, available at <http://www.visa.ca/chip/merchants/benefitsofchippin/index.jsp> (last visited Oct. 15, 2015) (describing how fraud related to lost and stolen payment cards in the UK decreased by more than half since chip and PIN was adopted there in 2004); see also Submission of Visa Worldwide, Visa AP (Australia), and MasterCard Asia/Pacific to the Australian Competition & Consumer Commission in support of Authorisations A91379 & A91380 (Aug. 30, 2013), "Security of Chip and PIN vs. Signature," pp. 1-2, available at <http://registers.accc.gov.au/content/index.phtml?itemID=1120516&display=submission> (last visited Oct. 15, 2015) (affirming "[t]he Applicants' view is that chip and PIN is a significantly more secure form of [customer verification method] than signature").

³See NRF Survey, available at <https://nrf.com/sites/default/files/Documents/Chip-and-Pin%20Consumer%20Survey%20One-Pager%2009-16-2015%20REV.pdf>.

venting fraud than signature transactions and lead to “increased checkout speed and improved customer service.”⁴

The consumer experience is a priority for any small business. So it is difficult for me to accept that the card networks and banks are promoting chip-without-PIN when chip-and-PIN is widely proven to benefit consumers—and the numbers show that consumers want it.

Unfortunately, there are many problems with the transition to EMV. This is not surprising given the fact that the card companies developed the transition timeline and requirements without input from merchants and consumers. Beyond the expense and unreasonable timeliness, the most frustrating aspect of the transition is that it will fall short of the fraud-prevention and consumer protection benefits it could easily achieve. Retailers want strong security—and we’ve been paying to try to get it—but transitioning to unproven chip-without-PIN technology threatens to have a significant negative impact on small businesses like mine. My company will continue to shell out money to pay for fraud several times over despite investing hundreds of thousands of dollars in the card networks’ chosen technology. That is wrong and needs to change.

⁴“The Benefits of Chip and PIN for Merchants,” *available at* <http://www.visa.ca/chip/merchants/benefitsofchippin/index.jsp> (last visited Oct. 18, 2015) (including a statement that “using a PIN is 2 to 4 seconds faster than obtaining a signature...”); *see also* “The Importance of PIN,” *available at* <http://www.visa.ca/chip/cardholders/importance-of-pin/index.jsp> (last visited Oct. 18, 2015) (Visa advertises to consumers on its website in Canada (where chip and PIN has been implemented), in a section titled “The Importance of PIN,” that “PIN transactions are easy.”)

Testimony of

Mr. Art Potash

Chief Executive Officer for Potash Markets

On Behalf of the

Food Marketing Institute

Before the

House Small Business Committee

Hearing on

The EMV Deadline and What it Means for Small Businesses: Part II

October 21, 2015

Washington, D.C.

Introduction:

Good Morning Chairman Chabot, Ranking Member Velázquez and members of the Committee. My name is Art Potash and I am the CEO of Potash Markets in Chicago, Illinois. My family has owned and operated grocery stores in the Chicago area for 65 years. We currently employ 140 people. The Potash family tradition continues today of helping our customers fulfill their culinary passions and lead healthier and more fulfilling lives. We enjoy strong customer loyalty to our local grocery stores and strive to meet our customers' preferences and demands, from the food we sell to their peace of mind when using their credit cards to pay in our stores. I appreciate the opportunity to speak to you today about steps my company has taken to migrate to EMV and the challenges we have faced along the way. It is incredibly important that this committee, Congress and the American Consumer fully understands how EMV is being implemented here in the United States, what its potential benefits are, how it is different than it has been done globally, and the unique challenges small merchants are facing in meeting these standards.

About the Food Marketing Institute:

Food Marketing Institute proudly advocates on behalf of the food retail industry. FMI's U.S. members operate nearly 40,000 retail food stores and 25,000 pharmacies, representing a combined annual sales volume of almost \$770 billion. Through programs in public affairs, food safety, research, education and industry relations,

FMI offers resources and provides valuable benefits to more than 1,225 food retail and wholesale member companies in the United States and around the world. FMI membership covers the spectrum of diverse venues where food is sold, including single owner grocery stores, large multi-store supermarket chains and mixed retail stores. For more information, visit www.fmi.org and for information regarding the FMI foundation, visit www.fmifoundation.org.

Decision and Experience Migrating to EMV:

As Visa's witness explained in the prior hearing, their company did not place an explicit mandate on merchants to migrate to EMV. Instead, Visa, MasterCard and the other card brands announced that any merchants who did not migrate to EMV would have additional fraud costs placed upon them. This would be in addition to fraud costs we already pay in interchange fees and chargebacks. As the other witnesses have and will testify today, each merchant then had to make the business decision of if the added cost of fraudulent cards would outweigh the cost of upgrading their point of sale systems to EMV.

After studying the costs and benefits, including providing the most robust security for our customers' payment card data, we decided, like the majority of the grocery industry, to work to migrate our stores to EMV. As you can imagine, upgrading to EMV in my business is not as easy as buying a \$49.99 Square reader. Our cash registers and credit card readers are more complex, providing for credit, debit, SNAP transactions, coupons and returns, among other features such as our customer loyalty card program, and ties into a network that requires substantial upgrades on both the front end and back end to be EMV-compliant as well as PCI-compliant.

Additionally, like many others, I am in the business of selling groceries and I rely on third party vendors to actually perform these upgrades and interface with the other links in the chain. A small business such as mine does not have the resources to perform the programming to convert our system to EMV or the financial wherewithal to own our own switch. Instead, we rely on and pay our merchant acquirer, in our case Worldpay, to make this happen for us so we can focus on selling groceries.

During the first hearing, the panel frequently referred to the \$49.99 Square EMV solution, or a \$100 off the shelf EMV point of sale reader. That characterization innately did not reflect the true needs and perspective of the merchant community. The true cost estimates in the United States for merchants to convert to EMV runs into the billions of dollars. Even the conservative estimate of \$8 billion for merchants did not appear to consider back end costs as well as man hours and potential downtime while upgrading the system. This is a huge investment and cost on all merchants large and small.

In May, we installed all new EMV point of sale devices in two of our three stores at a cost of \$1,000 per lane. For the two stores, this means an upgrade cost of \$8,000 just to conduct EMV-compliant payment transactions. This is a large investment to our small

business, but we are willing to make it to protect our customers and hopefully get a reduction in fraud and our fraud expenses.

While we now have EMV readers in our stores, we are not yet EMV-compliant and are now facing a holiday season exposed to greater fraud liability as we wait for our merchant acquirer to complete our transition. Currently, our acquirer has estimated they will be ready to upgrade our back end software by the end of November at best.

The Cost of EMV and Card Acceptance for Merchants Moving Forward:

This is an investment we made without much incentive from the card brands. Unlike the issuing banks who were enticed to issue chip cards with the promise of seeing their fraud costs reduce, merchants were pushed to do so under the threat of seeing their costs increase. This is particularly difficult for us to accept when we already pay the highest interchange fees in the modern world in the name of fraud costs. Visa, MasterCard and the other card brands have defended charging American merchants \$71 billion a year in interchange fees as a way of offsetting the cost of fraud. If a portion of this fee is assessed because of fraud, those fees should be reduced if fraud is reduced. Unfortunately, as we heard in the first hearing, Visa has no plans to pass any savings along to merchants. We hope that will change and we hope that the Federal Reserve will see to it that this changes.

The card networks have pushed merchants and encouraged issuers to migrate to EMV here in the United States under the guise of reducing fraud, but without promising to share any of those savings. As a small business I compete every day with other food retailers from the large box chains to other specialty markets, these fees restrict my ability to grow and compete and are a cost that I have absolutely no control over. The rule with Visa and MasterCard has basically always been "take it or leave it" with regards to their operating rules and fee structure, placing merchants of all sizes, particularly small ones, at their mercy.

In addition, consider the following historical trend. Retail food companies operate at razor thin margins due to the competitive nature of retail food industry. Our profit margin has never hit or exceeded 2% in the 60 years we have been collecting data. When food retailers have realized savings through efficiencies due to technological advancements and other cost saving measures the net profit for businesses in the retail food industry has remained at below 2% and savings have been passed along to the customer. This is further assurance that if retailers realize savings from reduced fraud those savings will also be passed along to the customer.

There is a Need for Competition:

As you can see from above the grocery industry is incredibly competitive, with even the largest company holding less than a 15% market share. We in the grocery industry all compete for customers every day with competitive prices, value and incentives to keep our customers and earn new ones. The credit card market is inherently

different with the top two brands, Visa and MasterCard holding over 85% of the market. These brands do not compete for merchant acceptance. They compete for banks to issue their cards, and they compete by promising revenues from sources such as interchange fees they charge to merchants who accept their cards. There is no competition with the brands to garner merchant acceptance. So while the grocery customer has more opportunities to save money as my store competes with others for their business, retailers have virtually no options as customers of the credit card companies to reduce their costs.

A Missed Opportunity to Truly Improve Card Security:

I would be remiss if I failed to address the issue of PIN authentication. Every point of sale in our stores is PIN-enabled. PIN is a proven safety measure that has been adopted globally, everywhere but here in the United States. Historically, the card companies have rolled out EMV as “chip and PIN” technology. So, not only are they verifying that the card is legitimate, they are also confirming that the person presenting the card is authorized to use it. Unfortunately, here in the United States, the card companies have rolled out an untested model of “chip and choice” as they call it. They left it up to the issuing banks to decide whether to issue PINs.

I have been a bit mystified by the card brands’ and banks’ defense of not requiring PIN. One of the most interesting is the argument that the PIN is a static number and once compromised is useless. They instead argue for biometric authentication or continue to defend the useless signature method. This argument has a real problem. If your PIN is somehow compromised, or you forget it, you can go to your bank and reset it. Many current and former government employees will tell you, once your fingerprint or other biometric is compromised, there is no “reset.” You cannot go and change your thumbprint; it truly is static. So I think the “PIN is static” argument has a few holes in it.

We all agree, technology and industry are evolving and improvements are made every day, but here is what we know today: PIN works today. It reduces fraud, period.

I think it is important to respond to a question that was raised during the first hearing regarding PIN. A member asked if the card companies allowed merchants to require a PIN. The answer is no. We can prompt for PIN, but the current Visa and MasterCard operating rules that every merchant must adhere to or face fines or loss of the privilege of accepting their cards will not allow a merchant to require a PIN for a transaction that does not include cashback on a card, even if it is PIN-enabled. This is a very important note to make. Banks require a PIN when the customer uses its ATM to withdraw money, but will not allow me the same privilege when a customer is making a purchase in my store.

A Federal Data Security and Breach Notification Law:

Another issue that was raised during the first hearing that deserves a merchant response is the bank and credit union witnesses

support for H.R. 2205 the Data Security Act of 2015. To be clear, Potash Markets is committed to protecting our customers' payment card data. Gross mischaracterizations that merchants are not committed to protecting our customers' payment card data and that we are not held to any standards is simply not true. In addition to the various state laws merchants must comply with, the Federal Trade Commission has taken an active interest in holding merchants liable for not adequately protecting customer data with over fifty cases already pursued. Where we agree with the banks and credit unions, grocers and other merchant groups would like to replace the patchwork of state laws with one federal standard. Where we differ, is how that federal law should work. Unfortunately, H.R. 2205 in its current form takes a standard that was written specifically for the banks and puts it on any and all that accept credit and debit cards. Our desire is to work with the bill drafters to create a final product that will allow for the flexibility necessary that will allow for a small business such as me to take necessary steps to protect data, but tailor it specifically to my business needs, not unnecessarily opening me up to liability and heavy handed enforcement without merit. We all have the common goal of protecting customer data, but that should be addressed with fair and narrowly written legislation not punitive overly restrictive requirements.

What Merchants Are Expecting Next in Electronic Payments:

Another piece that was raised during the first hearing has taken on even more greater importance in the last week. The Visa witness shared a perspective on merchants having an option to "turn on" the near field communication (NFC) technology on the new EMV readers. She offered it as a feature and option but not required or mandated. Unfortunately, this past week we got a glimpse of what we should expect next. Last week, merchants in the United Kingdom were informed by their merchant acquirers that Visa and MasterCard will not mandate that they turn on and accept NFC transactions. This is something many American merchants have feared was coming next. By requiring that all merchants turn on and accept NFC transaction, Visa and MasterCard have moved to lock in their mobile payments solution, and effectively block other entrants into the market. They will ensure that every merchant accept their solution before any others can make it to market. By eliminating further competition in that space, Visa and MasterCard are moving to guarantee their dominance in the market continues. It is also important to note, it is not as easy as flipping a switch for a merchant to "turn on" their NFC function. This will require further certification, cost and investment.

Conclusion:

As you can see, there is a great deal more to EMV on the merchant side than buying a \$100 piece of hardware off the shelf, or opting for Square's \$49.99 solution. There is significantly more investment, dependence on vendors and long-term repercussions to be considered. As mentioned earlier in my testimony, we are doing

all of this on an untested model of chip and choice, versus the proven fraud reducing solution of chip and PIN technology. All of this affects merchants of all sizes, but as this committee knows very well, these challenges can be greatly magnified when it comes to small businesses.

In conclusion, Potash Markets has made significant investments and is committed to migrate to EMV. Unfortunately, we find ourselves in the unenviable place of waiting for our providers to get us across the finish line, while we face a busy holiday season with the threat of higher fraud liability over our heads. I greatly appreciate the committee's interest in this very important issue, and look forward to answering your questions.

**Testimony of Edmund Mierzwinski
U.S. PIRG Consumer Program Director**

at a hearing on

**“The EMV Deadline and What it Means for Small
Businesses: Part II”**

Before the House Small Business Committee

Honorable Steve Chabot, Chair

21 October 2015

Testimony of Edmund Mierzwinski, U.S. PIRG Consumer Program Director at a hearing on “The EMV Deadline and What it Means for Small Businesses: Part II”, Before the House Small Business Committee, 21 October 2015

Chair Chabot, Representative Velázquez, members of the committee, I appreciate the opportunity to testify before you on the important matter of consumer data security and the implications of the 1 October 2015 EMV liability change for small businesses and their consumer customers. Since 1989, I have worked on data privacy, among other financial issues, for the U.S. Public Interest Research Group. The state PIRGs are non-profit, non-partisan public interest advocacy organizations that take on powerful interests on behalf of their members.

Summary:

Chip and PIN is Safer than Chip and Signature: Since the 1970s, the U.S. credit card, and later, also debit card, markets relied on magnetic stripe verification technology. To better deter “card-present” or in-person fraud, Canada and Europe switched to much stronger Chip and PIN technology over a decade ago. The U.S. is finally transitioning to Chip cards, although most banks are expected to offer the less robust Chip and Signature, rather than Chip and PIN, cards. Chips prevent information from your card from being transferred into merchant computers and prevent your card from being cloned. PINs prove you are not an imposter. Note that neither technology will deter online fraud, only in-person (card-present) fraud.

To accelerate the belated conversion of the U.S. system at least to Chip, or EMV (Europay, Mastercard and Visa), systems, the Payment Card Industry (PCI) security standards body made a scheduled liability change on 1 October 2015. As of that date, merchants face greater fraud liability if they have not installed card readers that accept Chip cards. Banks that have not issued Chip cards retain greater liability. Gas stations have a longer implementation period.

Banks Make More Money From Signature Transactions: While the banks have a polished narrative making other explanations as to “Why Chip, not Chip and PIN?”, it really comes down to one factor: Visa and Mastercard have long functioned as a cartel with market power to drive traffic to their own payment networks—which are signature-enabled, not PIN enabled. They earn much higher merchant “swipe” or interchange fees. As merchant witnesses will explain, they already faced significant liability as well as are limited in their choices by card network rules. All consumers, including cash customers, pay more at the store and more at the pump due to these rules, which drive traffic to the higher-cost, yet riskier signature platforms, not PINs, quite simply because Visa and Mastercard profit more from transactions on those platforms. In either case, lower-income cash customers end up subsidizing more-affluent rewards card customers because merchants bake the cost of swipe fees into their prices.

We urge no preemptive federal action on data breaches:

For several years Congress has considered national data breach notification legislation. Nearly every proposal I have seen, including numerous bills before this Congress, contains an onerous Trojan Horse provision. Even though most federal bills provide only extremely limited consumer protections, they broadly preempt state data security and consumer protection laws. Data breaches can result in numerous types of harms yet the bills do not recognize all the harms. The states have already implemented data breach notice laws that are working well.

I will discuss each of these points in greater detail in the following discussion.

Discussion:

The transition to Chip cards means merchant data breaches will no longer act as such a treasure trove of account numbers and expiration dates for existing account fraud. The Chip technology prevents the transfer of the full card number and expiration date to the merchant, who will receive only a one-time transaction code. The Chip cannot be cloned, meaning counterfeit cards usable in Chip “dip” readers cannot be created from the information available after a data breach. Of course, many cards will be backward-compatible for some time (still have a magnetic stripe to be “swiped”) but these will be used at fewer and fewer card readers over time, limiting their value to bad guys going forward.

However, we remain concerned that most U.S. banks and credit unions are expected to convert only to Chip cards, not fully to Chip and PIN cards,, which are safer for consumers and preferred by merchants, both of whom will still face the problems of stolen Chip cards in a “Chip and Signature” world. Chips prove your card is not a clone; PINs prove you are not an imposter.

So far, we are only aware of one bank, upstate New York’s First Niagara Bank, that’s gone beyond Chip and Signature and is rolling out the more robust Chip and PIN.¹ Positively, President Obama ordered last year that all U.S. issued credit cards and all U.S. agency card readers by Chip-and-PIN.²

When debit or credit card **numbers** only are stolen, such as in a breach, consumer protections are quite strong, although debit card customers may face cash flow problems while they wait for the bank to conduct a reinvestigation and replace money in their accounts. However, when debit cards themselves are lost, debit card customers face much greater liability, much more quickly.

The December 2013 Target stores breach ultimately affected some 110 million customers and Target accountholders. The first tranche of some 40 million customers had their card numbers skimmed or “scraped” off the card reader software and made con-

¹ See Matt Glynn, “First Niagara rolling out Chip-and-PIN cards”, Buffalo News, 30 September 2015 <http://www.buffalonews.com/business/first-niagara-rolling-out-Chip-and-pin-cards-20150930>

² See Fred Williams, “Obama puts federal might behind Chip-and-PIN card security Social Security, other federal payment cards to switch in 2015,” <http://www.creditcards.com/credit-card-news/obama-federal-backs-Chip-and-pin-1282.php>

sumers vulnerable to existing account fraud, forcing numerous banks to replace cards.³ But the Target breach was only one in a long series of breaches, and an increase in card fraud generally, that had led to the proposal for the EMV card switch.

Target and other breached merchants should be held accountable for their failure to comply with applicable security standards but that does not mean they are 100% responsible for breaches. Merchants, and their customers, had been forced by the card monopolies to use an unsafe payment card system that relies on obsolete magnetic stripe technology, buttressed by a constantly changing set of so-called PCI standards to compensate for the inherent flaws of the underlying, ancient stripe tech.

Increasing consumer protections under the Electronic Funds Transfer Act (EFTA), which applies to debit cards, to the gold standard levels of the Truth in Lending Act, which applies to credit cards, should be a step taken by Congress. While EFTA provides for zero liability if a consumer notifies her bank within 60 days after her debit card number, but not her card, is stolen, she still faces the stigma of bouncing checks and cash flow problems while waiting for the bank to reinstate her funds, which is a problem for consumers living from paycheck to paycheck. But if a debit card is stolen, liability by law of up to \$500 begins accrue if the bank is not notified within 2 days. After 60 days, liability could be greater than \$500 and could include funds taken from linked accounts. Conversely, the Truth In Lending Act grants credit card customers very strong protections in all cases, plus, no money is ever removed from your own bank account by credit card thieves.

The card networks continued to use an obsolete 1970s magnetic stripe technology well into the 21st century because, as oligopolists, they wanted to extract greater rents from the system. When the technology was solely tied to credit cards, where consumers enjoyed strong fraud rights and other consumer protections by law, this may have been barely tolerable.

But when the big banks and credit card networks asked consumers to expose their bank accounts to the unsafe signature-based payment systems, by piggybacking once safer PIN-only ATM cards onto the signature-based system after re-branding them as “debit” cards, the omission became unacceptable. The vaunted “zero-liability” promises of the card networks and issuing banks are by contract, not law. Of course, the additional problem any debit card fraud victim faces is that she is missing money from her own account while the bank conducts an allowable reinvestigation for ten days or more, even if the bank eventually lives up to its promise.⁴ Further, the contractual promises I have seen contain asterisks and exceptions, such as for a consumer who files more than one

³After the thieves rooted around inside the Target mainframe for some time, they obtained phone numbers and email addresses for many more consumers with Target accounts. These data could then be used for social engineering or “phishing” attacks designed to obtain the additional information—Social Security Numbers and birth dates—that make it possible to commit “new account identity theft.”

⁴Compare some of the Truth In Lending Act’s robust credit card protections by law to the Electronic Funds Transfer Act’s weak debit card consumer rights at this FDIC website: http://www.fdic.gov/consumers/consumer/news/cnfall09/debit_vs_credit.html

dispute in a year. Congress should also provide debit and prepaid card customers with the stronger billing dispute rights and rights to dispute payment for products that do not arrive or do not work as promised that credit card users enjoy (through the Fair Credit Billing Act, a part of the Truth In Lending Act).⁵

Further, the card networks' failure to upgrade, let alone enforce, their PCI security standards, despite the massive revenue stream provided by consumers and merchants through swipe, or interchange, fees, is yet another outrage by the banks and card networks.

Merchants that accept credit and debit cards are already subject to a set of fees and a set of rules. The full "swipe fee" includes a small fee paid to the network, a small fee paid to the merchant's bank and a very large interchange fee paid to the consumer's bank. Merchants also pay third-party processing fees. A portion of the interchange fee is already allocated to fraud prevention. Merchant swipe fees (deducted from the payments they receive from banks) could range from about 1% for a "classic" debit card to 3.5% or more for an airline rewards credit card. (The fee schedules are complex and the fee often includes a flat fee plus a percentage of the cost of the transaction. Different merchant classes pay different fees.)

Rules include both the security compliance standards set by the Payment Card Industry (PCI) process that led to this liability shift as well as to additional complex network rules.⁶

Incredibly, the Federal Reserve Board's rule interpreting the Durbin amendment to the 2010 Dodd-Frank Wall Street Reform and Consumer Protection Act, which limited swipe fees on the debit cards of the biggest banks, also provided for additional fraud revenue to the banks in several ways. Even though banks and card networks have routinely passed along virtually all costs of fraud to merchants in the form of chargebacks, the Federal Reserve rule interpreting the Durbin amendment allows for much more revenue. So, not only are banks and card networks compensated with general revenue from the ever-increasing swipe fees, but the Fed allows them numerous additional specific bites of the apple for fraud-related fees.⁷

Under the Fed's Durbin rules the amount of this additional compensation is as follows: banks can also get 5 basis points per transaction for fraud costs, 1.2 cents per transaction for transaction monitoring, and 1 cent per transaction for the fraud prevention adjustment. Again, this is in addition to merchants already paying chargebacks for fraud as well as PCI violation fines, plus litigation

⁵For a detailed discussion of these problems and recommended solutions, see Hillebrand, Gail (2008) "Before the Grand Rethinking: Five Things to Do Today with Payments Law and Ten Principles to Guide New Payments Products and New Payments Law," *Chicago-Kent Law Review*: Vol. 83, Iss. 2, Article 12, available at <http://scholarship.kentlaw.iit.edu/cklawreview/vol83/iss2/12>

⁶These network rules set by Visa and Mastercard, as well as by Discover and American Express, have been the subject of a variety of public and private antitrust lawsuits over many years but are not directly the subject of this testimony.

⁷See 77 Fed. Reg. page 46264 (August 3, 2012), available at <http://www.gpo.gov/fdsys/pkg/FR-2012-08-03/pdf/2012-18726.pdf>.

damages, and, now, possible additional direct costs of fraud for failing to install Chip readers.

Unfortunately, without PINs, the EMV transition will not provide merchants and consumers the level of protection against fraud that they both seek.

Further, while most news discussion and bank political advertising related to the Durbin amendment focuses on bank complaints about both the reduced revenue stream and the merchants' purported failure to pass along savings, it is important to understand that other provisions of the amendment were also important. For example, the Durbin amendment makes it easier for merchants to "signal" to consumers that certain payment methods, including the use of alternative networks, cost them less and are preferred. Of course, the least-costly networks are generally PIN-based, but most consumers, thanks to banks only moving partway, will not have PIN cards.

We are only aware of one bank, upstate New York's First Niagara Bank, that's gone beyond Chip and Signature and is rolling out the more robust Chip and PIN.⁸ Positively, President Obama ordered last year that all U.S. issued credit cards and all U.S. agency card readers be Chip-and-PIN.⁹

This month, the FBI offered but then immediately "walked back" a recommendation to consumers and merchants that Chip and PIN is better than Chip and Signature. As Senator Durbin asked in a letter to FBI director Comey last week:

"The revisions to the FBI advisory raise significant questions about whether current EMV security technology is adequately protecting consumers and whether the FBI is taking appropriate steps to warn against and deter payment card fraud involving lost or stolen cards," said Durbin. "Did representatives of the American Bankers Association contact the FBI between the issuance of the October 8 advisory and the release of the revised advisory? If so, did the American Bankers Association request that the advisory's recommendations for consumers and merchants to use PINs be removed?"¹⁰

The committee should join Senator Durbin in asking Director Comey these questions.

We believe that if Congress act in the payment card security, it should take steps, as the President did, to encourage all users to use the highest possible existing standard. Congress should also take steps to ensure that additional technological improvements and security innovations are not blocked by actions or rules of the

⁸See Matt Glynn, "First Niagara rolling out Chip-and-PIN cards", Buffalo News, 30 September 2015 <http://www.buffalonews.com/business/first-niagara-rolling-out-Chip-and-pin-cards-20150930>

⁹See Fred Williams, "Obama puts federal might behind Chip-and-PIN card security Social Security, other federal payment cards to switch in 2015," <http://www.creditcards.com/credit-card-news/obama-federal-backs-Chip-and-pin-1282.php>

¹⁰See "Durbin Calls for FBI to Explain Walkback of Consumer Protection Advisory Regarding Security Features on Credit and Debit Cards," 15 October 2015, <http://www.durbin.senate.gov/newsroom/press-releases/durbin-calls-for-fbi-to-explain-walkback-of-consumer-protection-advisory-regarding-security-features-on-credit-and-debit-cards>

existing players. In general, this means proposing or encouraging a technology-neutral performance standard.

If Congress does choose to impose higher standards, then it must also impose them equally on all players. For example, current legislative proposals may unwisely impose softer regimes on financial institutions subject to the weaker Gramm-Leach-Bliley rules than to merchants and other non-financial institutions.

Further, as most observers are aware, Chip technology will only prevent the use of cloned cards in card-present (Point-of-Sale) transactions. It is an improvement over obsolete magnetic stripe technology in that regard, yet it will have no impact on online transactions, where fraud volume is much greater already than in point-of-sale transactions. Experiments, such as with “virtual card numbers” for one-time use, are being carried out online. It would be worthwhile for the committee to inquire of the industry and the regulators how well those experiments are proceeding and whether requiring the use of virtual card numbers in all online debit and credit transactions should be considered a best practice.

Congress should not enact any federal breach law that preempts state breach laws or, especially, preempts other state data security rights or protections: In 2003, when Congress, in the FACT Act, amended the Fair Credit Reporting Act, it specifically did not preempt the right of the states to enact stronger data security and identity theft protections.¹¹ We argued that since Congress hadn’t solved all the problems, it shouldn’t prevent the states from doing so.

From 2004-today, 46 states enacted security breach notification laws and 49 state enacted security freeze laws. Many of these laws were based on the CLEAN Credit and Identity Theft Protection Model State Law developed by Consumers Union and U.S. PIRG.¹²

A security freeze, not credit monitoring, is the best way to prevent identity theft. If a consumer places a security freeze on her credit reports, a criminal can apply for credit in her name, but the new potential creditor cannot access your “frozen” credit report and will reject the application. The freeze is not for everyone, since you must unfreeze your report on a specific or general basis whenever you re-enter the credit marketplace, but it is only way to protect your credit report from unauthorized access.¹³

The other problem with enacting a preemptive federal breach notification law is that industry lobbyists will seek language that not only preempts breach notification laws but also prevents states from enacting any future security laws, despite the 2003 FACT Act example above.

¹¹ See “conduct required” language in Section 711 of the Fair and Accurate Credit Transactions Act of 2003, Public Law 108-159. Also see Hillebrand, Gail, “After the FACT Act: What States Can Still Do to Prevent Identity Theft,” Consumers Union, 13 January 2004, available at <http://consumersunion.org/research/after-the-fact-act-what-states-can-still-do-to-prevent-identity-theft/>

¹² See <http://consumersunion.org/wp-content/uploads/2013/02/model.pdf>

¹³ <http://defendyourdollars.org/document/guide-to-security-freeze-protection>

Simply as an example, S. 961 (Carper) includes sweeping preemption language that is unacceptable to consumer and privacy groups and likely also to most state attorneys general:

SEC. 6. Relation to State law.

No requirement or prohibition may be imposed under the laws of any State with respect to the responsibilities of any person to—

- (1) protect the security of information relating to consumers that is maintained, communicated, or otherwise handled by, or on behalf of, the person;
- (2) safeguard information relating to consumers from—
 - (A) unauthorized access; and
 - (B) unauthorized acquisition;
- (3) investigate or provide notice of the unauthorized acquisition of, or access to, information relating to consumers, or the potential misuse of the information, for fraudulent, illegal, or other purposes; or
- (4) mitigate any potential or actual loss or harm resulting from the unauthorized acquisition of, or access to, information relating to consumers.

Such broad preemption will prevent states from acting as first responders to emerging privacy threats. Congress should not preempt the states. In fact, Congress should think twice about whether a federal breach law that is weaker than the best state laws is needed at all.

I would also note that most federal breach proposals define harm very narrowly to financial harm. As we have seen with the latest breaches of health insurance companies, tax preparation firms and the IRS itself, and now even the U.S. OPM, harms from data breaches have gone far beyond existing account fraud or even new account identity theft to include theft of medical services, theft of tax refunds and the reputational and physical threat harms that could result from the OPM breach of security clearance files, including fingerprints.¹⁴ Just a few weeks ago, a national consumer reporting agency, Experian, was even breached, although it states that its credit reports on 200 million Americans were not affected.¹⁵

In addition, most federal proposals have a weak notice requirement with a risk “trigger” based on a narrow definition of harm. The better state breach laws, starting with California’s, require breach notification if information is presumed to have been “acquired.” The weaker laws allow the company that failed to protect the consumer’s information in the first place to decide whether to tell them, based on its estimate of the likelihood of identity theft or other harm, but no other harms.

¹⁴I discussed the issue of broad harms and narrow protections in detail here in my blog (24 June 2015): <http://uspirg.org/blogs/eds-blog/usp/more-i-hear-about-opm-data-breach-less-i-know-except-its-bad>

¹⁵News release, “PIRG, Others Ask CFPB, FTC to Investigate Experian/T-Mobile Data Breach,” 8 October 2015, <http://www.uspirg.org/news/usp/pirgs-others-ask-cfpb-ftc-investigate-experiant-mobile-data-breach>

Only an acquisition standard will force data collectors to protect the financial information of their trusted customers, accountholders or, as Target calls them, “guests,” well enough to avoid the costs, including to reputation, of a breach.

Congress Should Allow For Private Enforcement and Broad State and Local Enforcement of Any Law It Passes:

The marketplace only works when we have strong federal laws and strong enforcement of those laws, buttressed by state and local and private enforcement.

Many of the data breach bills I have seen specifically state no private right of action is created. Such clauses should be eliminated and it should also be made clear that the bills have no effect on any state private rights of action. Further, no bill should include language reducing the scope of state Attorney General or other state-level public official enforcement. Further, any federal law should not restrict state enforcement only to state Attorneys General. For example, in California not only the state Attorney General but also county District Attorney and even city attorneys of large cities can bring unfair practices cases.

Although we currently have a diamond age of federal enforcement, with strong but fair enforcement agencies including the CFPB, OCC and FDIC, that may not always be the case. By preserving state remedies and the authority of state and local enforcers, you can better protect your constituents from the harms of fraud and identity theft.

Review Title V of the Gramm-Leach-Bliley Act and its Data Security Requirements:

The 1999 Gramm-Leach-Bliley Act imposed data security responsibilities on regulated financial institutions, including banks. The requirements include breach notification in certain circumstances.¹⁶ Congress should ask the regulators for information on their enforcement of its requirements and should determine whether additional legislation is needed. The committee should also recognize that compliance with GLBA should not constitute constructive compliance with any additional security duties imposed on other players in the card network system as that could lead to a system where those other non-financial-institution players (merchants) are treated unfairly.

Conclusion:

In conclusion, consumers will benefit from lower fraud risks by the transition to a Chip card regime but the banking industry deserves to be called out for imposing higher Chip reader costs on merchants without also further reducing their fraud risk by rolling out Chip and PIN instead of Chip and signature cards. The liability shift is a big stick, added to numerous other “fee and rule sticks” that the banks already use to extract fees and maintain market

¹⁶ See the Federal Financial Institutions Examination Council’s “Final Guidance on Response Programs: Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice,” 2005, available at <http://www.fdic.gov/news/news/financial/2005/fil2705.html>

power; but the carrot of reducing fraud even further by going with “best available” technology rather than “best for banks” technology would have been a better solution.

I would also note two other impacts on consumers from the transition. First, as the FTC has noted, the rollout is confusing and scam artists are taking advantage of the October 1 date to create new scam pitches to consumers.¹⁷ Another problem I have heard of, although not confirmed, is one that may be faced by consumers traveling in Europe who encounter unattended fare machines that may require a PIN at all times.

Thank you for the opportunity to provide the Committee with our views. We are happy to provide additional information to Members or staff.

¹⁷See FTC blog of 19 October 2015, “Scam du jour: Chip card scams,” <http://www.consumer.ftc.gov/blog/scam-du-jour-Chip-card-scams>

Statement for the Record*On behalf of the***American Bankers Association****Consumer Bankers Association****Credit Union National Association****Financial Services Roundtable****Independent Community Bankers of America****National Association of Federal Credit Unions***before the***Small Business Committee****United States House of Representatives**

Chairman Chabot, Ranking Member Velazquez, and members of the Committee, the ABA, CBA, CUNA, ICBA and NAFCU on behalf of the 14,000 banks and credit unions of all sizes that are taking on criminal hackers by issuing payment cards with highly secure “EMV” microchips, we appreciate the Committee’s interest in the transition to the next generation in payments security and respectfully request that this statement be made part of the record for today’s hearing.

An estimated 575 million so-called “chip” cards will be issued by year-end, millions of merchants will be on the road to implementation, and the U.S. marketplace will be significantly safer at the cash register for our nation’s consumers. EMV (or “chip”) technology makes stolen card numbers useless to thieves if they try to create counterfeit cards, and address the lion’s share of today’s fraud for in-store (or “card-present”) transactions. The rollout of chip or “EMV” technology demonstrates how the financial services and retail industries can and must work together to better protect consumers.

While the Committee’s October 7th hearing was helpful in highlighting some of the issues around EMV, we want to share additional information based on some of the questions raised at the hearing to assist you in preparation for today’s hearing.

First, the move to chip technology has been underway for quite some time. The transition to EMV began in 2011, and card networks, banks and credit unions, merchant bank processors, and the merchants themselves have been involved in implementing the transition since that time. Indeed, many merchant banks have worked with small businesses to identify ways to upgrade payment terminals at low- or no-cost. Merchants are our customers—we want them to succeed.

Second, consumers will benefit greatly from this transition. After the major data breaches at big box stores, like Target and Home Depot, tens of millions of account numbers were posted online, which could have easily been used to create counterfeit cards. In response, banks and credit unions reissued millions of cards at an unprecedented pace in order to protect consumers from fraud. Going forward, chip cards greatly reduce the fraud risks stemming from such breaches by generating a one-time code for each transaction, eliminating the possibility that those chip cards can be counterfeited and used at another store. Once chip cards fully replace the magstripe—the *U.S. has already issued the most chip cards of any country in the world*—and merchants turn on their chip card readers, counterfeit cards will become a lot harder to create.

Third, merchants are fully empowered to protect themselves from any increased liability as part of this transition. Once merchants install chip card readers and turn them on, liability returns to the financial institution. Chip card readers are available for very reasonable prices. Depending upon the vendor and type of upgrade needed, it can be zero or as little as \$49, which makes it easy for merchants of all sizes to protect their customers at minimal cost. Moreover, liability shifts only for accounts that are chip-enabled—so if the card issuer has not done its part, it bears the risk. This is a private sector incentive to encourage adoption and better consumer protections.

Fourth, the “PIN argument” is a smokescreen used by retail trade groups to deflect attention from the high profile retail data breaches at big box stores over the past few years and their underlying causes. Rather than coming together to improve internal data security practices, the retail trades are fixating on a PIN technology that fights a small and declining share of today’s fraud and which would have been meaningless in breaches like those at Target and Home Depot. The reality is that if a merchant is EMV enabled and has their card readers turned on, they have the same protections whether PIN is used or not. Instead of fighting, we should embrace ideals like H.R. 2205, the Data Security Act of 2015, introduced by Representatives Neugebauer (R-TX) and Carney (D-DE), to apply meaningful and consistent data protection for consumers nationwide.

Finally, an attempt is being made to interject one of the most controversial parts of the Dodd-Frank Act—the price controls of the Durbin Amendment—into the chip card discussion. The fact is that banks and credit unions annually spend billions on innovation in payment security in order to stay ahead of the thieves. We are pioneering cutting-edge solutions—like the “tokenization” technologies used in Apple Pay and Samsung Pay, end-to-end encryption, and biometric authenticators—to protect transactions wherever they take place. That forward-looking approach to “tomorrow’s threats” today should be the focus of our collective discussions.

Ultimately, the only way to protect our data is to stay ahead of the ever-changing criminal element through joint efforts. The security of our payments system impacts all of us and the payments

system will only be secured if everybody—banks, credit unions, payment networks, retailers and consumers—work together to fight a common enemy.

Sincerely,

American Bankers Association
Consumer Bankers Association
Credit Union National Association
Financial Services Roundtable
Independent Community Bankers of America
National Association of Federal Credit Unions



October 21, 2015

Chairman Steve Chabot
House Committee on Small Business
2371 Rayburn House Office Building
Washington, D.C. 20515

Ranking Member Nydia Velázquez
House Committee on Small Business
2302 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Chabot and Ranking Member Velázquez,

The Food Marketing Institute¹ commends you for holding the hearing entitled, “*The EMV Deadline and What it Means for Small Businesses: Part II.*” It is essential that the merchant’s voice is heard on this most important issue. FMI was particularly pleased that you invited one of our board members, Art Potash of Potash Markets, a family-owned, three store company in Chicago, Illinois to testify about his company’s experience migrating to EMV. Art is an active member of the FMI Independent Operator Committee and will be a great addition to your panel. In addition to the perspective that Art Potash offers, FMI would like to offer this letter highlighting what we have learned from our members in the supermarket industry regarding EMV migration here in the United States for the Committee record.

For the past four years, since Visa and then MasterCard and the other card brands announced their roadmaps for migrating to EMV in the United States, EMV migration has been a top priority for our members. Through the FMI Electronic Payment Systems Committee, we have held numerous interactive EMV migration sessions, starting four years ago and continuing through the first half of 2015. We engaged with experts involved in EMV migration in Europe on the food retail side to get their perspective and lessons learned. Unfortunately, the card brands have not rolled out EMV in the U.S. in the same or a similar fashion to the implementation globally.

Need For PIN-Enabled Cards

¹ Food Marketing Institute proudly advocates on behalf of the food retail industry. FMI’s U.S. members operate nearly 40,000 retail food stores and 25,000 pharmacies, representing a combined annual sales volume of almost \$770 billion. Through programs in public affairs, food safety, research, education and industry relations, FMI offers resources and provides valuable benefits to more than 1,225 food retail and wholesale member companies in the United States and around the world. FMI membership covers the spectrum of diverse venues where food is sold, including single owner grocery stores, large multi-store supermarket chains and mixed retail stores. For more information, visit www.fmi.org and for information regarding the FMI foundation, visit www.fmifoundation.org.

One of the most notable differences between EMV in the U.S. and globally is the lack of the requirement that credit cards be PIN-enabled. As you know, a PIN, a personal identification number, is unique to the user of the card and is a simple way of verifying the individual presenting the card is indeed authorized to use it. PIN is universally considered to be far safer than a signature verification method that does nothing to ensure the person using the card is actually authorized to do so. The migration to EMV chip and PIN was successful in other parts of the world because the card networks and issuing banks recognized the effectiveness of PIN in reducing lost and stolen credit card fraud and made it a practice to issue cards with a PIN and then give merchants an incentive to make the investment in reducing fraud via lower card acceptance costs.

Unfortunately, in the U.S. the card brands have taken the unprecedented path of allowing for “chip and choice,” where issuing banks can make the business decision whether to issue PIN-enabled cards or stick with the fraud-prone signature cards. Unfortunately, the vast majority of banks so far have chosen the easier route of issuing signature cards instead of the safer PIN-enabled cards – the path suggested by the White House and chosen for federal government payment and benefit cards.

This is particularly frustrating for the grocery industry, which is already fully enabled to accept PIN authentication. Every day, customers enter their PIN to get cashback at our registers or to use government issued benefit cards for programs like SNAP and WIC. Grocers are ready and willing to utilize the more robust PIN authentication, but unfortunately the card brands have held firm against requiring banks to issue these safer cards, leaving us with the untested “chip and choice” option as the one most widely seen in the current marketplace.

We are also challenged to find logic in the issuers’ new line of arguing that a PIN is not safe because it is a static number that does not change, and if it were to become compromised is useless. They argue that because the PIN is set, and not dynamic it is not secure and instead say they want to look forward to using biometrics such as fingerprints. This is an interesting argument, as anyone who has been issued a debit card with a PIN knows; you can go to your bank and change it if you think it may have been compromised or if you forgot the number. However, as many former and current government employees recently learned from the Office of Personnel Management breach, once your thumb print is compromised in a data breach, you cannot “reset” it like a PIN. We agree, technology is advancing, and new solutions are coming to the market, but arguing PINs are not secure because they are “static” is inherently flawed. Additionally, we know PIN works today to reduce fraud. It is tried and proven on debit cards, government benefit cards and credit cards in Europe and around the world. The card brands should move as they have in other countries to require banks to PIN-enable all cards and allow a merchant to require a PIN for transactions.

FMI would also like to respond to a point that was raised during the first hearing when a member asked about whether a merchant could require a customer to enter a PIN. We felt that the question went unanswered, and would like to point out that under the existing operating rules, a merchant may not require a PIN for a transaction that does not include cashback under the current Visa, MasterCard and other brands' operating rules. The operating rules allow a merchant to prompt for PIN, but a customer may bypass the prompt and choose only a signature. The card brands require all merchants, small, medium and large, to comply with all of their operating rules or face extraordinary fines for non-compliance. It is worth noting that the card brands and banks continue to see the value in PINs as they still require a customer to enter a PIN in order to withdraw money from their ATMs. All we ask is that merchants be given the opportunity to utilize the same level of authentication.

As an interesting point, some of our members have reported that because the card brands decided to change course and go with "chip and choice" unlike the traditional and proven "chip and PIN" solution it complicated the migration here in the U.S. and slowed the process down. Instead of taking what was used in the United Kingdom and throughout Europe, Canada and elsewhere as a starting point, they had to provide additional specification for "chip and choice."

In short, PINs are proven and available in the market today. While issuers may have decided to make the business decision against issuing PIN cards, it was not in the name of security. For your reference, we have included a very informative article from the September 2015 issue of *Digital Transactions*, "EMV's Signature Moment." In this article, the author outlines three business drivers that led banks to decide not to issue PINs, first their concern of consumer experience and if a bank put a PIN on a card, the consumer would pick the one without it instead. The article also explained that there lacked a return on investment for banks, and finally the actual bank's processor capabilities and need for upgrading to process larger PIN volumes. Nowhere did the article suggest that banks chose not to issue PIN due to security concerns.

The Continued Cost of Accepting Credit and Debit Cards

Another important point that was raised during the last hearing was the anticipated savings from fraud reduction post-EMV migration, and if Visa expected to share any of those savings with the merchants. Unfortunately, Visa reaffirmed merchants' fears that they currently have no plans to share savings seen from reduction in fraud due to EMV migration with merchants. American merchants paid the card brands over \$71 billion in interchange fees in 2013. The card brands have long defended these extraordinary fees saying they needed them to help cover their fraud costs. So now, when they are pushing merchants to invest billions to upgrade to EMV in the name of fraud reduction, they are not planning to share savings resulting from the investment in

EMV equipment and cards, leaving U.S. merchants to still pay an overwhelming bulk of global interchange fees.

When you couple this with the pure lack of financial incentive beyond facing additional fraud liability for EMV migration, American merchants are clearly going to be paying more, not less. Visa, MasterCard and the card brands have continually said EMV is not mandated on merchants; it is their choice. First, supermarket retailers have been investing for years in payments security. We want our customers' transactions and data to be secure. This is true, however, merchants are left with the choice of not investing significant funds and being saddled with new additional fraud costs on top of what they are already paying in interchange and chargebacks, or invest heavily to upgrade to EMV. This is different from the choice banks were given. Banks could choose to maintain their current fraud liabilities and not issue chip cards, or chose to issue chip cards and be rewarded with lower fraud costs. The banks were given a clear financial incentive, where merchants were given threat of higher costs if they did not.

FMI's members have invested significant funds in EMV-compliant terminals, software interfaces and certification to migrate to EMV and hopefully a more secure system here in the United States. Many of our members are now EMV certified and are currently accepting EMV cards today. Many more are still in the process, having purchased EMV-compliant terminals months ago, yet still waiting for certification of the links to their merchant acquirer and other vendors. In the meantime, until the other links are ready, they will continue to accept cards and potentially face higher fraud liability heading into the busy holiday season.

What to Expect Next

Last week, merchants in the United Kingdom were notified by their merchant acquirers that the Near Field Communications (NFC) "option" they have had since migrating to EMV will no longer be an option; it will now be required. Visa and MasterCard are now mandating that all merchants turn on and become NFC certified in the United Kingdom. This is a very different message from what the committee heard from Visa during the last hearing. The witness from Visa testified that NFC was a feature and was optional for merchants as they migrated to EMV. American merchants were essentially put on notice last week that mandatory NFC is what we should expect next.

The card brands have chosen NFC as their mobile solution, but there are others already in the market, and more that can still come. Some mobile solutions utilize reading QR codes; others use blue tooth technology or the existing magnetic stripe reading solution that is already in the point of sale device. By mandating NFC, the brands are ensuring that all point of sales take their solution even if a merchant would prefer to use a QR or blue tooth solution instead.

This mandate is particularly troubling as merchants look toward mobile payments solutions and the opportunity for real competition entering into the payments space. With Visa and MasterCard mandating merchants turn on and accept all NFC transactions, they are essentially ensuring their hold on the market requiring that merchants accept their mobile solution universally. This is something American merchants had feared. It is also important to note, beyond the policy concerns that the mandate brings, there is always a cost associated with it as well. It is not as easy as flipping a switch for a merchant to start taking NFC transactions. They will have to again invest funds into both programming and certification. These are costs that will certainly come out of the merchant's pocket, yet again without any promise of a rate reduction.

The Payments Realm Needs Real Competition

Currently, Visa and MasterCard hold over 85% of that credit and debit card market. In dollar terms, Visa and MasterCard debit, credit and prepaid cards that were issued in the United States generated over \$3.6 trillion in purchase volume in 2014. That kind of market power has worked to block others from entry and threaten to do the same when our economy migrates to mobile payments.

Conversely, the grocery industry is incredibly competitive with large and small merchants competing every day to earn and keep customers. They do this by keeping costs low, in fact, the grocery industry averages around 1% profit margin every year. Merchant customers have benefited from lower costs, greater benefits and numerous options on where to spend their grocery dollars.

It is time the credit card industry became an open and competitive market, where efficiencies and competition drive down the cost for merchants to accept these payments. Mobile offers the possibility of new players and greater competition, but it is essential that the card brands not be allowed to put up road blocks preventing others from entering into the market.

The Need for Federal Data Security Legislation

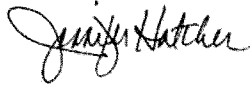
Finally, FMI would like to respond to the bank and credit union witness's call during the last hearing for support for H.R. 2205, the Data Security Act of 2015. FMI has members operating in every state, many operating in multiple states. Currently, merchants must comply with a myriad of state data security and breach notification laws. Grocers and many other merchant groups have long advocated for a federal data security and breach notification standard to replace the various and sometime conflicting state laws. However, we strongly believe that any federal law must be written carefully to ensure it is not overly burdensome on any of the industries covered by the law. Unlike the Gramm-Leach Bliley law that was written specifically for one industry, the banks and financial institutions, this federal law would cover anyone who accepts a

credit or debit card --including a dentist, political campaign, grocer and charitable cause. All of those entities have unique needs and what works for a grocer with regard to breach notification would be different than what a dentist or charitable cause should do. FMI and our members advocate for a federal law that allows for the flexibility to tailor standards to meet the needs of a particular business in a particular industry. Unfortunately, as written, H.R. 2205 attempts to place standards that were written specifically for banks and those in the financial services industry on anyone who accepts a credit or debit card, including the smallest merchant. FMI has engaged with the bill drafters and is actively working to reach a compromise that will take into consideration the Federal Trade Commission's existing authority reflect the various needs of all industries covered under the legislation. Additionally, a basic premise for breach notification should be that the breached party notifies. There may be places for an exception, but merchants believe that the underlying standard should be that the breached party notifies. In its current form, H.R. 2205 does not meet that standard and could leave small businesses liable for notifying customers about a breach when they were not even the one breached. FMI is committed to working with the bill drafters to address these challenges and ensure that any legislation is written to properly cover all industries without unnecessarily subjecting anyone, particularly small businesses, to unnecessarily liability or punitive overly burdensome actions.

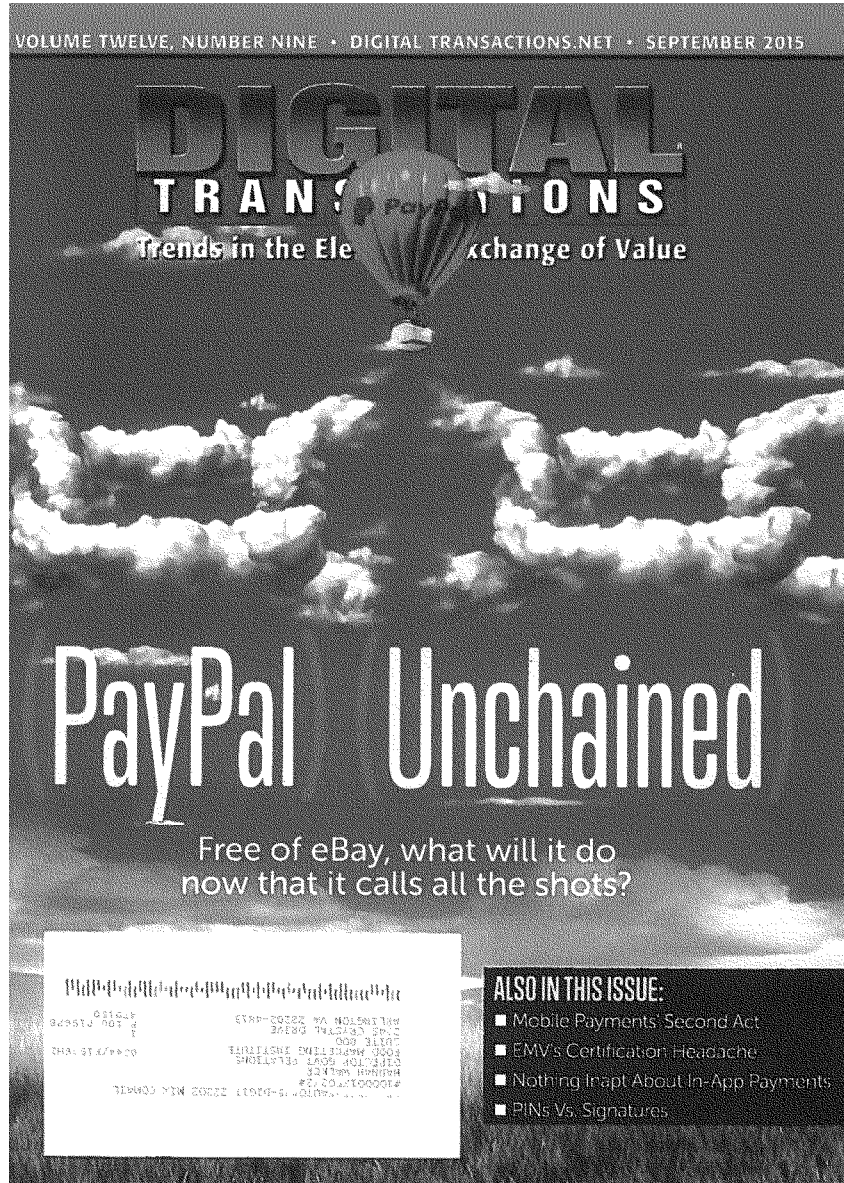
Conclusion

Clearly it is a pivotal time for merchants in the payments sphere. We commend the committee for taking an active interest in EMV migration and how America's small businesses are faring under the card brands' initiatives. Thank you for your interest in this matter, and we look forward to working with you on EMV and other issues moving forward.

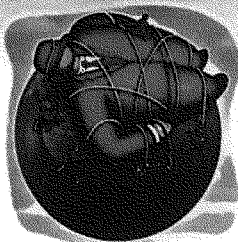
Sincerely,



Jennifer Hatcher
Senior Vice President
Government and Public Affairs



SECURITY

September 2015 *digital* transactions

EMV's Signature Moment

By John Stewart

While PINs are more secure, signatures are by far card issuers' preferred authentication method for U.S. EMV credit cards. Why?

By the time you read this, the big EMV deadline will be anywhere from 15 to 30 days away. Yet, with so little time remaining, the effort to implement the chip card standard in the United States faces any number of hurdles, from certification headaches (page 16) to lagging merchant terminal adoption.

And you can add one more item to the list: the PIN vs. signature controversy. It's one of the oldest disputes in the brief history of American EMV, but merchants are still wrangling with banks over the question of whether chip cards should be universally issued with PINs—credit cards as well as debit.

Merchant groups have aggressively pushed PINs for EMV ever since the card networks got serious four years ago about the conversion from magnetic-stripe cards to the chip card standard. But most U.S. financial institutions that have issued EMV credit cards so far have overwhelmingly done so with the signature authentication so familiar from decades of card swiping.

In fact, issuers are so entrenched in signature-card issuance that some experts see signature-based EMV credit cards as a *fait accompli*. "This train has left the station whether it'll be PIN or signature," says Nick

Holland, a senior analyst at Javelin Strategy & Research, Pleasanton, Calif., who follows EMV.

But the issue simply won't die, even with a crucial deadline only weeks away.

By card-network rules, merchants that aren't prepared to accept EMV chip cards by Oct. 1 will assume liability for any counterfeit fraud (some networks add lost-and-stolen fraud) losses—losses that are currently borne by the issuer. The issuer will continue to bear those losses if the card involved isn't EMV-compliant.

'Worthless' Signatures

Despite the deadline's proximity, merchant groups aren't giving up. They're adamant that PINs are surer barriers to fraud than signatures, which a number of retail executives over the years have dismissed as "worthless."

Their latest salvo came out in July in the form of a survey of 84 IT decision makers conducted in May and June by business-technology company Randstad Technologies. The study not only concluded PINs were superior to signatures, it all but called for an industry mandate that issuers adopt PINs. Nearly two-thirds of the respondents preferred PIN security for EMV.

"The majority (66 percent) believe chip and signature does not offer ample security and that PIN technologies

should be required," reads a Randstad summary of the survey results.

"If there's anything surprising in these numbers, it's that nearly six percent of respondents believe that mag-stripe technology offers sufficient security," summary continues. "That's a perspective that's been undercut on many occasions by costly security breaches to a number of prominent businesses."

Merchants are also questioning why they're spending so much time and money on EMV training and installations when their chip readers will end up accepting only signature-based credit cards.

"Retailers are investing billions to implement new chip-enabled card readers in stores nationwide. They're asking banks and credit unions to meet that commitment by issuing new chip cards with PINs," says the Arlington, Va.-based Retail Industry Leaders Association in a recent press release.

The retailer faction received further support this summer from no less a figure than a governor of the Federal Reserve Board.

"New approaches to authentication increasingly offer greater assurance and protection. Given the current technologies that we have at our disposal, we should assess the continued use of signatures as a means of authenticating card transactions," said Fed governor Jerome H. Powell in a speech given late in June at a payments conference at the Kansas City Fed.

To be sure, some financial institutions have gone with something they refer to as "chip and choice," an approach by which they support online PIN authentication as well as signature.

A prominent example is Raleigh, N.C.-based State Employees Credit Union, the second largest credit union in the country. SECU issues all of its EMV credit cards with PINs and allows its cardholders to authenticate with either the PIN or a signature, says Leanne Phelps, senior vice president for card services.

So far, though, less than one-half of 1% of all of SECU's credit card transactions have been PIN-authenticated. And of the 120 million or so EMV cards U.S. financial institutions had issued by the start of the year, the great majority were credit cards requiring only a signature from the cardholder.

That number is expected to balloon to 600 million by the end of 2015, according to the EMV Migration Forum, an industry trade group. Most will still be credit cards, and no one's betting that any appreciable number of them will require a PIN.

'Pretty Stupid'

So, with merchants insisting on PINs for EMV, and with few doubting that PINs are more secure, why are banks and credit unions mostly issuing signature-based credit cards? The reasons are manifold, but fall into three broad categories: consumer experience, return on investment, and processor capability.

Experts cite consumer familiarity with signature-based credit cards—along with a dearth of consumer education about EMV—as a prime reason issuers are sticking with signature authentication.

They don't want to see their cards disfavored by consumers who aren't accustomed to memorizing and entering a PIN. Typically, if you forget your PIN, it's hard to start all over and use a signature. "If your card is suddenly harder to use, you lose top of wallet," notes Rick Oglesby, senior analyst at Double Dia-

mond Research, Centennial, Colo.

So, "issuers are defaulting to the method they know always works," says Louis Buccheri, an analyst at Auritemma Consulting Group, New York City.

Besides that, the type of fraud issuers are most concerned with is counterfeit fraud, which chip cards are pretty effective at preventing. Lost-and-stolen fraud, which PINs would prevent, comes to a much smaller total.

Indeed, of all card-fraud losses, 37% are attributable to counterfeit cards, compared to 14% for lost-and-

stolen cards, according to a study of 18 of the 40 largest issuers conducted in 2014 by Aite Group, a Boston-based research firm.

That makes it harder for issuers to justify investments in credit card operations to handle PIN resets, among other back-office changes. "Lost-and-stolen is the only thing PIN buys you (as an issuer). It was a pretty easy business case for chip-and-signature," says Julie Conroy, a senior analyst at Aite.


Finally, issuers that are supporting online PINs with EMV credit cards, like SECU, are doing so with in-house systems. Or they've signed up with a processor that can handle credit card PINs.

But it turns out some processors that handle card transactions on behalf of issuers haven't geared up for PINs on credit card transactions, say Conroy and other experts. "A lot of the [third-party] issuer systems on the credit card side are really pretty stupid," says Steve Mott, principal at Stamford, Conn.-based payments consultancy BetterBuyDesign.

How Long?

Most markets around the world that have adopted EMV, such as Canada and United Kingdom, are using offline PIN authentication (chart). In this configuration, the card relies on its embedded chip to match the PIN entered at the terminal with the encrypted PIN in the chip. But this method relies on a more powerful, and hence more expensive, chip.

That's another thing that makes EMV credit cards a more costly proposition for issuers. After all, they're also racing to get cards out the door, and not just because of the liability shift. They know that the last mag-stripe issuer will be the one on which the fraudsters will focus all their considerable resources.

Still, no one is ruling out EMV credit card PINs forever. The superiority of PINs over signatures can't be denied, after all, when cardholders catch on and start asking about the matter. It would just be nice to know how long that's going to take. 

How the World Verifies EMV

(Preferred methods)

Country or Region	Signature	Online PIN	Offline PIN
Asia ¹			
Australia		✓	
Bahrain			✓
Belgium			✓
Brazil			✓
Canada			✓
Estonia			✓
Finland			✓
France			✓
Germany	✓		
Ireland			✓
Italy	✓		
Kuwait			✓
Mexico	✓		
Netherlands			✓
New Zealand		✓	
Norway			✓
Poland			✓
Portugal	✓		
Qatar			✓
Russia	✓		
Saudi Arabia			✓
Slovakia			✓
Spain	✓		
Sweden			✓
Turkey	✓		
U.K.			✓
U.A.E.			✓

¹ Except Japan. Source: Aite Group

October 16, 2015

The Honorable Steve Chabot
Chairman
Committee on Small Business
Washington, D.C. 20515

The Honorable Nydia Velazquez
Ranking Member
Committee on Small Business
Washington, D.C. 20515

Dear Chairman Chabot and Ranking Member Velazquez:

On behalf of the 14,000 banks and credit unions of all sizes that are taking on criminal hackers by issuing payment cards with highly secure “EMV” microchips, we appreciate the Committee’s interest in the transition to the next generation in payments security. With an estimated 575 million so-called “chip” cards to be issued by year-end and millions of merchants on the road to implementation, the U.S. marketplace will be significantly safer at the cash register for our nation’s consumers.

As you know, EMV (or “chip”) technology makes stolen card numbers useless to thieves if they try to create counterfeit cards, and address the lion’s share of today’s fraud for in-store (or “card-present”) transactions. The rollout of chip or “EMV” technology demonstrates how the financial services and retail industries can and must work together to better protect consumers.

While the Committee’s October 7th hearing was helpful in highlighting some of the issues around EMV, we want to share additional information based on some of the questions raised at that hearing to assist you in preparation for the Committee’s next hearing on EMV.

First, the move to chip technology has been underway for quite some time. The transition to EMV began in 2011, and card networks, banks and credit unions, merchant bank processors, and the merchants themselves have been involved in implementing the transition since that time. Indeed, many merchant banks have worked with small businesses to identify ways to upgrade payment terminals at low- or no-cost. Merchants are our customers—we want them to succeed.

Second, consumers will benefit greatly from this transition. After the major data breaches at big box stores, like Target and Home Depot, tens of millions of account numbers were posted online, which could have easily been used to create counterfeit cards. In response, banks and credit unions reissued millions of cards at an unprecedented pace in order to protect consumers from fraud. Going forward, chip cards greatly reduce the fraud risks stemming from such breaches by generating a one-time code for each transaction, eliminating the possibility that those chip cards can be counterfeited and used at another store. Once chip cards fully replace the magstripe – *the U.S. has already issued the most chip cards of any country in the world* – and merchants turn on their chip card readers, counterfeit cards will become a lot harder to create.

Third, merchants are fully empowered to protect themselves from any increased liability as part of this transition. Once merchants install chip card readers and turn them on, liability returns to the financial institution. Chip card readers are available for very reasonable prices. Depending upon the vendor and type of upgrade needed, it can be zero or as little as \$49, which makes it easy for merchants of all sizes to protect their customers at minimal cost. Moreover, liability shifts only for accounts that are chip-enabled—so if the card issuer has not done its part, it bears the risk. This is a private sector incentive to encourage adoption and better consumer protections.

Fourth, the “PIN argument” is a smokescreen used by retail trade groups to deflect attention from the high profile retail data breaches at big box stores over the past few years and their underlying causes. Rather than coming together to improve internal data security practices, the retail trades are fixating on a PIN technology that fights a small and declining share of today’s fraud and which would have been meaningless in breaches like those at Target and Home Depot. The reality is that if a merchant is EMV enabled and has their card readers turned on, they have the same protections whether PIN is used or not. Instead of fighting, we should embrace ideas like H.R. 2205, the Data Security Act of 2015, introduced by Representatives Neugebauer (R-TX) and Carney (D-DE), to apply meaningful and consistent data protection for consumers nationwide.

Finally, an attempt is being made to interject one of the most controversial parts of the Dodd-Frank Act – the price controls of the Durbin Amendment - into the chip card discussion. The fact is that banks and credit unions annually spend billions on innovation in payment security in order to stay ahead of the thieves. We are pioneering cutting-edge solutions - like the “tokenization” technologies used in Apple Pay and Samsung Pay, end-to-end encryption, and biometric authenticators – to protect transactions wherever they take place. That forward-looking approach to “tomorrow’s threats” today should be the focus of our collective discussions.

Ultimately, the only way to protect our data is to stay ahead of the ever-changing criminal element through joint efforts. The security of our payments system impacts all of us and the payments system will only be secured if everybody—banks, credit unions, payment networks, retailers and consumers—work together to fight a common enemy.

Sincerely,

American Bankers Association
 Consumer Bankers Association
 Credit Union National Association
 Financial Services Roundtable

Independent Community Bankers of America
National Association of Federal Credit Unions

cc: Members of the House Committee on Small Business



National Grocers Association

U.S. House Small Business Committee

The EMV Deadline and What it Means for Small Business: Part II

On Behalf of the National Grocers Association

October 21, 2015

The National Grocers Association (NGA) appreciates the opportunity to submit comments for the record to the House Small Business Committee regarding the hearing scheduled for Wednesday, October 21, 2015 entitled *The EMV Deadline and What it Means for Small Business: Part II*.

NGA is the national trade association representing the retail and wholesale supermarkets that comprise the independent channel of the food distribution industry. An independent retailer is a privately owned or controlled food retail company operating a variety of formats. Most independent operators are serviced by wholesale distributors, while others may be partially or fully self-distributing. Some independents are publicly traded, but with controlling shares held by the family and others are employee owned. Independents are the true “entrepreneurs” of the grocery industry and dedicated to their customers, associates, and communities. The independent supermarket channel is accountable for close to 1% of the nation's overall economy and is responsible for generating \$131 billion in sales, 944,000 jobs, \$30 billion in wages, and \$27 billion in taxes. Many of our member companies are family owned and operated, privately held, and operate on a slimmer net profit margin than most small businesses, roughly 1%.

Following the previous hearing on the EMV liability shift earlier this month, NGA commends the Chairman for holding this hearing to shed light on the tremendous efforts that small businesses merchants, including independent supermarkets, have been making in order to become EMV compliant and the many challenges those businesses have faced on the road to implementation. NGA members are committed to doing their part to provide a safe and secure payments ecosystem for consumers, and support the move to chip-and-PIN (personal identification number) technology that has been a proven deterrent to fraud throughout Europe for more than 20 years as opposed to the less secure chip-and-signature EMV requirements currently being implemented in the United States.

EMV Background:

EMV stands for Europay, MasterCard, and Visa, the founding members of EMVCo in 1994. EMV technology includes payment cards that include an embedded computer chip that allows for increased security

through card validation and cardholder authentication that reduces fraud from lost and stolen cards. EMV technology has been the standard throughout much of the rest of the world for nearly 20 years, though EMV technology abroad has required a PIN (personal identification number) to be entered with each transaction, while in the United States, only a signature will be required, despite evidence that transactions involving a PIN are far more secure than a signature.

The transition to EMV in the United States began in 2011 when the payment brands introduced a pathway to adoption. The U.S. was scheduled to complete the transition to EMV on October 1, 2015. This transition included the implementation of chip-and-signature technology, requiring all merchants to update their point-of-sale (POS) card terminals in addition to the software that runs the front end systems, is estimated by some industry experts to cost between \$25-30 billion. For merchants that fail to meet the deadline for upgrading their POS card readers, the liability for fraud committed in their stores using chip-and-signature cards shifted to the merchant beginning on October 1, 2015. Throughout this process, merchant input and feedback has been stymied. The payment brands, as represented by EMVCo, have dictated the terms and conditions of the transition from the outset, and have been unresponsive to the needs of merchants who, many through no fault of their own, were not ready for the liability shift on October 1 due to delays in production or certification of card reader terminals.

Unfortunately, many NGA members invested tens of thousands or in some instances hundreds of thousands of dollars to upgrade hardware and software only to learn that their systems would not be ready by October 1, 2015 because necessary upstream certifications were severely backlogged. We understand some of the backlog was a result of a delay to provide necessary software code for parties to implement and certify by the deadline. As a result, thousands of independent grocers, including many small businesses, are now subject to this liability shift due to delays that were entirely out of their control. NGA strongly believes this is unacceptable and urges Visa and MasterCard to immediately take steps to ensure these merchants do not face losses as a result of the liability shift.

Though EMV has been the standard for nearly two decades throughout Europe and much of Asia, a more instructive comparison might be the Canadian transition to EMV which began only a few years ago. Visa was the first company in Canada to announce the conversion to chip-and-PIN in 2003, with other card issuers not far behind. Trials of the technology began in 2007 and lasted through 2009, with the first liability shift not set until October of 2010, a full 7 years after the shift was announced. In addition, the liability shift dates were moved on multiple occasions due to the fact that POS terminals were not available as a result of delays in production, meaning many larger merchants would be receiving their terminals in the months leading up to the holidays and would be forced to train their staff and customers on a new technology during the busiest time of year for merchants. Visa and MasterCard both changed their liability shift deadlines from October 2010 to March 2011 in

order to accommodate those merchants. Neither Visa nor MasterCard granted an extension of the liability shift in the U.S., despite a timeline that was several years shorter¹.

Challenges to Implementation:

Despite the best efforts of merchants large and small alike, many are facing significant challenges as they seek to implement the new EMV technology at the POS. The greatest challenge to implementation for merchants has been the aggressive timeline unilaterally set by Visa and MasterCard without input from merchants. While a timeline of four years may seem to be a reasonable amount of time to prepare for the liability shift and implement a new system, the timeline was much shorter in reality, and failed to adequately account for the massive demand the shift would place on terminal and software providers, and certification specialists. The initial timeline of four years was overly ambitious from the outset, as the Canadian rollout (featuring less than 1/10th the population of the U.S.) took more than ten years. In addition, delays in software manufacturing meant that the software to process debit transactions was not even available until April of 2015, meaning that any merchant that wanted to be able to accept debit transactions only had a six month timeframe during which to install their software, and have it tested in order to meet the October 1 deadline.

This truncated timeframe combined with the sheer volume of terminals that needed replacement (more than 12 million²) has resulted in massive delays for many merchants. Once merchants have received their POS terminals, often after 6-16 weeks of delays, there is still a lengthy process of programming, testing and certification before terminals are ready for customer use. Each of these steps can involve weeks of delays for various reasons. One of the most commonly reported issues facing merchants on their road to implementation is the severe shortage of terminal installation experts, which has led to significant delays in initial installation. A separate certification process for each of the major card brands (Visa, MasterCard, American Express and Discover) further complicates an already daunting process.

Many merchants report delays of weeks and even months at each stage of the transition. One NGA member reports that they are still waiting for software to be installed at the POS despite ordering their terminals in April 2015. In many instances technicians must physically install each PIN pad terminal at checkout lanes. With certification delays, piloting, and staff training, this store will likely be liable for fraudulent purchases for several months, despite beginning the transition more than 6 months in advance of the deadline.

Another NGA member operating more than 75 stores has had their terminals installed in their stores for nearly a year at an expense of more than \$400,000 and is still waiting to be provided with the certified software necessary to operate the terminals. Again, despite beginning the transition process more than a year in advance of

¹ EMV-USA. EMV Migration-Canada. Tracy Black. 02/15.

² Federal Reserve Bank of Chicago. Kandice Alter and Anna Neumann. 05/18/15.

the deadline, this company was not EMV compliant on October 1 and will be liable for any fraudulent purchases made with EMV cards until they can be provided with the software to activate their terminals.

There is a misconception that merchants can simply purchase an EMV enabled device at a Club store for \$50 - \$100 and be ready to accept EMV. The reality is that option is only realistic for the smallest merchants. The vast majority of NGA's members have "integrated" terminals, meaning the in-lane card terminal is electronically tied back to the POS system. Each of these card readers (hardware) costs approximately \$500 while also requiring specific software to be loaded, certified, and tested before being deployed to each check-out lane.

In addition, the vast majority of independent supermarkets have more than one checkout lane, often having 5-10 lanes depending on the size of the store-which can lead to a single store paying upwards of \$5000 per store just to upgrade the card reader terminals hardware. That \$5000 price tag also fails to account for the cost of software that needs to be installed in each POS terminal and the cost of labor during installation. Many businesses choose to install their new equipment after close of business, potentially necessitating businesses to pay overtime to employees who must stay past their normal work hours. These costs will vary from store to store, but to estimate that the cost of the transition will "average \$100," as indicated by the Electronic Transactions Association, is far short of the reality for even the smallest of grocery stores, and fails to account for additional costs beyond the necessary EMV hardware.

Current Standards:

The Payment Card Industry (PCI) data security standard (DSS) is applied to anyone that processes, stores or transmits credit card information-regardless of size. Founded by the five major payment brands (Visa, MasterCard, Discover, American Express and JCB), PCI has the ability to levy fines as high as \$100,000 per month against acquiring banks-with the full expectation that it will be passed down to the merchant. In addition to passing along fines, it is possible that an acquiring bank could terminate their relationship with the merchant altogether, or increase transaction fees.

PCI standards have been thrust onto merchants large and small without allowing the voice of the merchant to be heard in the process of creating those same standards. In addition, merchants have not been allowed to participate in the PCI executive committee that serves as the main governing body for PCI. For those merchants unfortunate enough to suffer a data breach that results in the loss of sensitive consumer data, it is likely that PCI will find the merchant to be out of compliance with the PCI DSS and will levy fines, despite the fact that the merchant had been certified as PCI compliant prior to the breach. For small businesses, this can be disastrous. According to the National Cyber Security Alliance, 60% of all small businesses that suffer a data breach will go out of business within six months.

More Security Needed:

As an integral part of the community that many customers visit more than once a week, independent supermarkets are fully committed to protecting their customers' personal information. NGA members continue to go above and beyond current security requirements such as PCI standards, by investing millions of dollars towards instituting end-to-end encryption, tokenization, and further exploring current best practices and emerging technologies that will allow them to better safeguard customer data.

Unfortunately, card-issuing banks have chosen not to implement the full use of chip-and-PIN technology in the United States, instead opting for the less-secure chip-and-signature. According to the United States Federal Reserve, chip-and-PIN technology is over 700 percent³ more secure than chip-and-signature and yet banks have chosen a half-measure move to chip-and-signature at the expense of the merchant. In addition to the Federal Reserve, the Federal Bureau of Investigation (FBI) recently put out a statement recommending that consumers use a PIN with their new chip card, as PIN provides greater security than signature verification. The FBI later released a revised statement on EMV that omitted the PIN recommendation; reports indicated that upon releasing the statement, the FBI received pressure from the American Bankers Association to revise their alert.

According to a recent survey conducted by the National Retail Federation, 62% of consumers would prefer to be issued chip-and-PIN cards, and 63% believe that chip-and-PIN provides more security than simple chip-and-signature⁴. While banks contend that consumers would balk at the idea of having to remember another PIN number, NRF's survey indicated that 83% of consumers would consider it worthwhile to remember another PIN in exchange for greater security. Despite consumer and merchant interest in chip-and-PIN technology, card-issuing banks have opted for less security-putting consumers and merchants at risk.

Banks have shown a willingness to adopt the less-secure signature option during the EMV transition where they can pass on liability for fraudulent charges to merchants. However, when it comes to making withdrawals from automatic transaction machines (ATMs), banks have been using PINs to verify the identity of their customers since the inception of the ATM in 1967. This is due to the fact that banks bear 100% of the liability for fraudulent transactions that occur at the ATM. If banks require customers to use PINs in order to access their funds through an ATM as a result of the added security that a PIN provides, it should serve as an endorsement for chip-and-PIN as a best practice among all members of the payments chain.

High-profile breaches in the last few years have greatly increased the level of awareness for the public and merchant community alike with regard to payment security, as the cost of fraud has skyrocketed from \$23

³ "2011 Interchange Fee Revenue, Covered Issuer Costs, And Covered Issuer And Merchant Fraud Losses Related To Debit Card Transactions," 3/5/13

⁴ Chip-and-PIN Consumer Survey One-Pager. 09/16/15.

billion in 2013 to \$32 billion in 2014⁵. While the U.S. has seen its incidents of fraud increase, Canada saw its fraud reduced by 40% from 2011-2012 once chip-and-PIN was instituted⁶, while the EU has seen an 80% reduction in fraud since its transition to chip-and-PIN EMV⁷. With a proven track record of preventing fraud in multiple regions throughout the globe, there is little reason to not institute chip-and-PIN in the U.S.

NGA Position:

The National Grocers Association (NGA) fully supports all efforts to make the payments chain more secure. However, NGA believes that industry should make use of every available technology in order to protect consumer information; including, chip-and-PIN technology, tokenization, end to end encryption, and other advanced security measures that would better ensure that consumer information remains safe throughout the payment chain.

Though NGA supports efforts to promote security throughout the payments chain, we believe that the transition to EMV would have been smoother with a higher level of cooperation and communication between all concerned parties. The input of small merchants was not accepted throughout the transition process, and as a result, many were not able to meet the liability shift deadline on October 1 and are now subjected to a fraud liability shift through no fault of their own. NGA calls on the card networks and issuing banks to provide a “safe harbor” for these merchants.

We look forward to continuing a constructive dialog with the Committee on these issues and others important to the independent supermarket channel, and appreciate the opportunity to present our views on the EMV liability shift and its effects on small businesses. Thank you for the opportunity to submit these comments.

Sincerely,



Greg Ferrara
Vice President, Public Affairs
National Grocers Association

⁵ Reuters. \$32 Billion Lost by Retailers to Credit Card Fraud—SmartMetric Brings Biometric Technology to Credit Card. 02/17/15.

⁶ Chase Paymentech Solutions. 2012.

⁷ Discover Financial Services. 2013.



805 15th St, NW Suite 708 | Washington, DC 20005
 TEL 202.650.5100 | Fax 202.650.5118 | www.technet.org

October 19, 2015

The Honorable Steve Chabot
 Chairman
 House Committee on Small Business
 2361 Rayburn House Office Building
 Washington, D.C. 20515

The Honorable Nydia Velazquez
 Ranking Member
 House Committee on Small Business
 B-343C Rayburn House Office Building
 Washington, D.C. 20515

Dear Chairman Chabot and Ranking Member Velazquez,

On behalf of TechNet, the bipartisan network of innovation economy CEOs and senior executives, I am writing to offer our perspective ahead of your committee's October 21 hearing, *The EMV Deadline and What it Means for Small Businesses: Part II*.

As the committee considers the impact the EMV deadline has on small business, TechNet encourages the committee to carefully consider the dynamic and evolving nature of the payments system marketplace. We also caution the committee against any effort that would have the effect of mandating the use of specific security or payment technologies. We believe that government mandates in this space would hinder the rapid rate of new payment innovations that are coming to market, especially in mobile wallet solutions that leverage new tools to authenticate payments and enhance security.

Technological innovation drives today's economic growth. TechNet member companies are creating jobs, deploying robust security solutions, and developing creative products that improve the lives of Americans each and everyday. However, when any type of technological solution is cemented in law, innovation is impeded. We urge you and your committee members to consider this concern during your upcoming hearing on the EMV deadline.

TechNet commends the committee for its interest in the EMV deadline and welcomes the opportunity to work with the committee and its members on this issue.

Sincerely,

Mike Ward
 Vice President, Federal Policy and Government Relations
 TechNet

cc: Members of the House Committee on Small Business